

Fortinet Network Security Professional NSE4 Exam Questions with VCE and PDF for Free Download from PassLeader (Question 201 - Question 225)

PassLeader just published the NEWEST Fortinet NSE4 exam dumps! And, PassLeader offer two types of the NSE4 dumps -- NSE4 VCE dumps and NSE4 PDF dumps, both VCE and PDF contain the NEWEST NSE4 exam questions, they will help you PASSING the Fortinet NSE4 exam easily! Now, get the NEWEST NSE4 dumps in VCE and PDF from PassLeader --

<http://www.passleader.com/nse4.html> (562 Q&As Dumps)

What's more, part of that PassLeader NSE4 dumps now are free --

https://drive.google.com/open?id=0B-ob6L_QjGLpWVVnQl8wTTd0NW8

QUESTION 201

You wish to create a firewall policy that applies only to traffic intended for your web server. The server has an IP address of 192.168.2.2 and belongs to a class C subnet. When defining the firewall address for use in this policy, which one of the following addressing formats is correct?

- A. 192.168.2.0 / 255.255.255.0
- B. 192.168.2.2 / 255.255.255.0
- C. 192.168.2.0 / 255.255.255.255
- D. 192.168.2.2 / 255.255.255.255

Answer: D

QUESTION 202

If a FortiGate unit has a dmz interface IP address of 210.192.168.2 with a subnet mask of 255.255.255.0, what is a valid dmz DHCP addressing range?

- A. 172.168.0.1 - 172.168.0.10
- B. 210.192.168.3 - 210.192.168.10
- C. 210.192.168.1 - 210.192.168.4
- D. All of the above.

Answer: B

QUESTION 203

A FortiGate unit can act as which of the following? (Select all that apply.)

- A. Antispam filter
- B. Firewall
- C. VPN gateway
- D. Mail relay
- E. Mail server

Answer: ABC

QUESTION 204

Which of the following components are contained in all FortiGate units from the FG50 models and up? (Select all that apply.)

- A. FortiASIC content processor.
- B. Hard Drive.
- C. Gigabit network interfaces.
- D. Serial console port.

Answer: AD

QUESTION 205

Which of the following methods can be used to access the CLI? (Select all that apply.)

- A. By using a direct connection to a serial console.
- B. By using the CLI console window in Web Config.
- C. By using an SSH connection.
- D. By using a Telnet connection.

Answer: ABCD

QUESTION 206

The command structure of the FortiGate CLI consists of commands, objects, branches, tables, and parameters. Which of the following items describes user?

- A. A command.
- B. An object.
- C. A table.
- D. A parameter.

Answer: B

QUESTION 207

The command structure of the CLI on a FortiGate unit consists of commands, objects, branches, tables and parameters. Which of the following items describes port1?

- A. A command.
- B. An object.
- C. A table.
- D. A parameter.

Answer: C

QUESTION 208

When creating administrative users, the assigned ____ determines user rights on the FortiGate unit.

Answer: access profile

QUESTION 209

Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function. An administrator must assign a set of UTM features to a group of users. Which of the following is the correct method for doing this?

- A. Enable a set of unique UTM features under "Edit User Group".
- B. The administrator must enable the UTM features in an identify-based policy applicable to the user group.
- C. When defining the UTM objects, the administrator must list the user groups which will use the UTM object.
- D. The administrator must apply the UTM features directly to a user object.

Answer: B

QUESTION 210

Which of the following items represent the minimum configuration steps an administrator must perform to enable Data Leak Prevention for traffic flowing through the FortiGate unit? (Select all that apply.)

- A. Assign a DLP sensor in a firewall policy.
- B. Apply one or more DLP rules to a firewall policy.
- C. Enable DLP globally using the config sys dlp command in the CLI.
- D. Define one or more DLP rules.
- E. Define a DLP sensor.
- F. Apply a DLP sensor to a DoS sensor policy.

Answer: ADE

QUESTION 211

Because changing the operational mode to Transparent resets device (or vdom) to all defaults, which precautions should an Administrator take prior to performing this? (Select all that apply.)

- A. Backup the configuration.
- B. Disconnect redundant cables to ensure the topology will not contain layer 2 loops.
- C. Set the unit to factory defaults.
- D. Update IPS and AV files.

Answer: AB

QUESTION 212

Which of the following statements best describes the proxy behavior on a FortiGate unit during an FTP client upload when FTP splice is disabled?

- A. The proxy will not allow a file to be transmitted in multiple streams simultaneously.
- B. The proxy sends the file to the server while simultaneously buffering it.

- C. If the file being scanned is determined to be infected, the proxy deletes it from the server by sending a delete command on behalf of the client.
- D. If the file being scanned is determined to be clean, the proxy terminates the connection and leaves the file on the server.

Answer: A

QUESTION 213

Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?

- A. TCP connection
- B. File attachments
- C. Message headers
- D. Message body

Answer: A

QUESTION 214

The FortiGate Web Config provides a link to update the firmware in the System > Status window. Clicking this link will perform which of the following actions?

- A. It will connect to the Fortinet support site where the appropriate firmware version can be selected.
- B. It will send a request to the FortiGuard Distribution Network so that the appropriate firmware version can be pushed down to the FortiGate unit.
- C. It will present a prompt to allow browsing to the location of the firmware file.
- D. It will automatically connect to the Fortinet support site to download the most recent firmware version for the FortiGate unit.

Answer: C

QUESTION 215

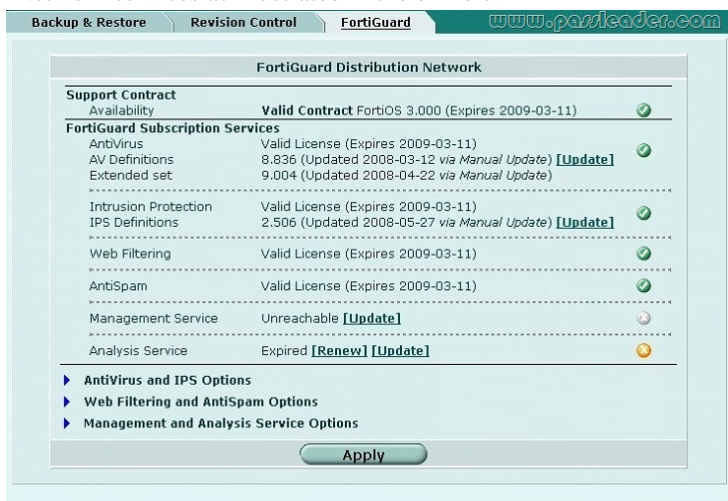
Which of the following statements correctly describes how a push update from the FortiGuard Distribution Network (FDN) works?

- A. The FDN sends push updates only once.
- B. The FDN sends package updates automatically to the FortiGate unit without requiring an update request.
- C. The FDN continues to send push updates until the FortiGate unit sends an acknowledgement.
- D. The FDN sends a message to the FortiGate unit that there is an update available and that the FortiGate unit should download the update.

Answer: D

QUESTION 216

Which of the following statements best describes the green status indicators that appear next to different FortiGuard Distribution Network services as illustrated in the exhibit?



- A. They indicate that the FortiGate unit is able to connect to the FortiGuard Distribution Network.
- B. They indicate that the FortiGate unit has the latest updates that are available from the FortiGuard Distribution Network.
- C. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate

unit.

D. They indicate that the FortiGate unit is in the process of downloading updates from the FortiGuard Distribution Network.

Answer: A

QUESTION 217

Data Leak Prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

- A. SNMP
- B. IPSec
- C. SMTP
- D. POP3
- E. HTTP

Answer: CDE

QUESTION 218

Which of the following statements are correct regarding Application Control?

- A. Application Control is based on the IPS engine.
- B. Application Control is based on the AV engine.
- C. Application Control can be applied to SSL encrypted traffic.
- D. Application Control cannot be applied to SSL encrypted traffic.

Answer: AC

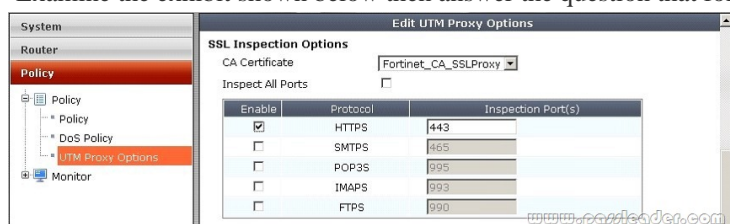
QUESTION 219

In addition to AntiVirus services, the FortiGuard Subscription Services provide IPS, Web Filtering, and ____ services.

Answer: antispam

QUESTION 220

Examine the exhibit shown below then answer the question that follows it.



Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following:

- A. FortiGate unit's encryption certificate used by the SSL proxy.
- B. FortiGate unit's signing certificate used by the SSL proxy.
- C. FortiGuard's signing certificate used by the SSL proxy.
- D. FortiGuard's encryption certificate used by the SSL proxy.

Answer: A

QUESTION 221

Shown below is a section of output from the debug command `diag ip arp list`.

```
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e state=00000004 use=4589 confirm=4589 update=2422 ref=1
```

In the output provided, which of the following best describes the IP address 172.20.187.150?

- A. It is the primary IP address of the port1 interface.
- B. It is one of the secondary IP addresses of the port1 interface.
- C. It is the IP address of another network device located in the same LAN segment as the FortiGate unit's port1 interface.

Answer: C

QUESTION 222

Review the output of the command `get router info routing-table all` shown in the Exhibit below; then answer the question following it.

```
STUDENT # 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 NSSA 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*   0.0.0.0/0 [10/0] via 10.200.1.254, port1
      [10/0] via 10.200.2.254, port2, [5/0]
C   10.0.1.0/24 is directly connected, port3
O   10.0.2.0/24 [110/101] via 172.16.2.1, Remote_1, 00:00:21
      [110/101] via 172.16.2.2, Remote_2, 00:00:21
C   10.200.1.0/24 is directly connected, port1
C   10.200.2.0/24 is directly connected, port2
C   172.16.1.1/32 is directly connected, Remote_1
C   172.16.1.2/32 is directly connected, Remote_2
C   172.16.2.1/32 is directly connected, Remote_1
C   172.16.2.2/32 is directly connected, Remote_2
```

Which one of the following statements correctly describes this output?

- A. The two routes to the 10.0.2.0/24 subnet are ECMP routes and traffic will be load balanced based on the configured ECMP settings.
- B. The route to the 10.0.2.0/24 subnet via interface Remote 1 is the active and the route via Remote 2 is the backup.
- C. OSPF does not support ECMP therefore only the first route to subnet 10.0.1.0/24 is used.
- D. 172.16.2.1 is the preferred gateway for subnet 10.0.2.0/24.

Answer: A

QUESTION 223

Review the IPsec phase1 configuration in the Exhibit shown below; then answer the question following it.

New Phase 1 [www.passleader.com](#)

Name: Remote_1
Comments: Write a comment... 0/255
Remote Gateway: Static IP Address
IP Address: 10.200.3.1
Local Interface: port1
Mode: Aggressive Main (ID protection)
Authentication Method: Pre-shared Key
Pre-shared Key: *****
Peer Options: Accept any peer ID
Advanced... (XAUTH, NAT Traversal, DPD)
 Enable IPsec Interface Mode
IKE Version: 1 2
Local Gateway IP: Main Interface IP Specify
P1 Proposal
1 - Encryption: AES192 Authentication: SHA1
DH Group: 1 2 5 14
Keylife: 28800 (120-172800 seconds)
Local ID: (optional)
XAUTH: Disable Enable as Client Enable as Server
NAT Traversal: Enable
Keepalive Frequency: 10 (10-900 seconds)
Dead Peer Detection: Enable

Which of the following statements are correct regarding this configuration? (Select all that apply).

- A. The phase1 is for a route-based VPN configuration.
- B. The phase1 is for a policy-based VPN configuration.
- C. The local gateway IP is the address assigned to port1.
- D. The local gateway IP address is 10.200.3.1.

Answer: AC

QUESTION 224

Review the output of the command config router ospf shown in the Exhibit below; then answer the question following it.

```
STUDENT (ospf) # show
config router ospf
  config area
    edit 0.0.0.0
    next
  end
  config network
    edit 1
      set prefix 10.0.1.0 255.255.255.0
    next
    edit 2
      set prefix 172.16.0.0 255.240.0.0
    next
  end
  config ospf-interface
    edit "R1_OSPF"
      set interface "Remote_1"
      set ip 172.16.1.1
      set mtu 1436
      set network-type point-to-point
    next
    edit "R2_OSPF"
      set cost 20
      set interface "Remote_2"
      set ip 172.16.1.2
      set mtu 1436
      set network-type point-to-point
    next
  end
  config redistribute "connected"
  end
  config redistribute "static"
  end
  config redistribute "rip"
  end
  config redistribute "bgp"
  end
  config redistribute "isis"
  end
  set router-id 0.0.0.1
end
```

Which one of the following statements is correct regarding this output?

- A. OSPF Hello packets will only be sent on interfaces configured with the IP addresses 172.16.1.1 and 172.16.1.2.
- B. OSPF Hello packets will be sent on all interfaces of the FortiGate device.
- C. OSPF Hello packets will be sent on all interfaces configured with an address matching the 10.0.1.0/24 and 172.16.0.0/12 networks.
- D. OSPF Hello packets are not sent on point-to-point networks.

Answer: C

QUESTION 225

Examine the static route configuration shown below; then answer the question following it.

```
config router static
edit 1
set dst 172.20.1.0 255.255.255.0
set device port1
set gateway 172.11.12.1
set distance 10
set weight 5
next
edit 2
set dst 172.20.1.0 255.255.255.0
set blackhole enable
set distance 5
set weight 10
next
end
```

Which of the following statements correctly describes the static routing configuration provided? (Select all that apply.)

- A. All traffic to 172.20.1.0/24 will always be dropped by the FortiGate unit.
- B. As long as port1 is up, all the traffic to 172.20.1.0/24 will be routed by the static route number 1. If the interface port1 is down, the traffic will be routed using the blackhole route.
- C. The FortiGate unit will NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
- D. The FortiGate unit will create a session entry in the session table when the traffic is being routed by the blackhole route.
- E. Traffic to 172.20.1.0/24 will be shared through both routes.

Answer: AC

Learning the PassLeader NSE4 dumps with VCE and PDF for 100% passing Fortinet certification --

<http://www.passleader.com/nse4.html> (562 Q&As Dumps)

BONUS!!! Download part of PassLeader NSE4 dumps for free --

https://drive.google.com/open?id=0B-ob6L_QjGLpWVVnQl8wTTd0NW8