Fortinet

NSE4-5.4 Exam

Fortinet Network Security Expert 4 Written Exam – FortiOS 5.4 Exam

Questions & Answers
Demo

Version: 13.0

Question: 1

A FortiGate interface is configured with the following commands:

```
config system interface
edit "port1"
config ipv6
set ip6-address 2001:db8:1::254/64
set ip6-send-adv enable
config ip6-prefix-list
edit 2001:db8:1::/64
set autonomous-flag enable
set onlink-flag enable
end
```

What statements about the configuration are correct? (Choose two.)

A. IPv6 clients connected to port1 can use SLAAC to generate their IPv6 addresses.
B. FortiGate can provide DNS settings to IPv6 clients.
C. FortiGate can send IPv6 router advertisements (RAs.)
D. FortiGate can provide IPv6 addresses to DHCPv6 client.

Answer: A,C

Question: 2

Which of the following Fortinet hardware accelerators can be used to offload flow-based antivirus inspection? (Choose two.)

A. SP3
B. CP8
C. NP4
D. NP6

Answer: A,B

Question: 3

Under what circumstance would you enable LEARN as the Action on a firewall policy?

A. You want FortiGate to compile security feature activity from various security-related logs, such as virus and attack logs.
B. You want FortiGate to monitor a specific security profile in a firewall policy, and provide recommendations for that profile.
C. You want to capture data across all traffic and security vectors, and receive learning logs and a report with recommendations.
D. You want FortiGate to automatically modify your firewall policies as it learns your networking behavior.

Answer: C

Question: 4

What methods can be used to deliver the token code to a user who is configured to use two-factor authentication? (Choose three.)

A. Code blocks
B. SMS phone message
C. FortiToken
D. Browser pop-up window
E. Email

Answer: B,C,E

Question: 5

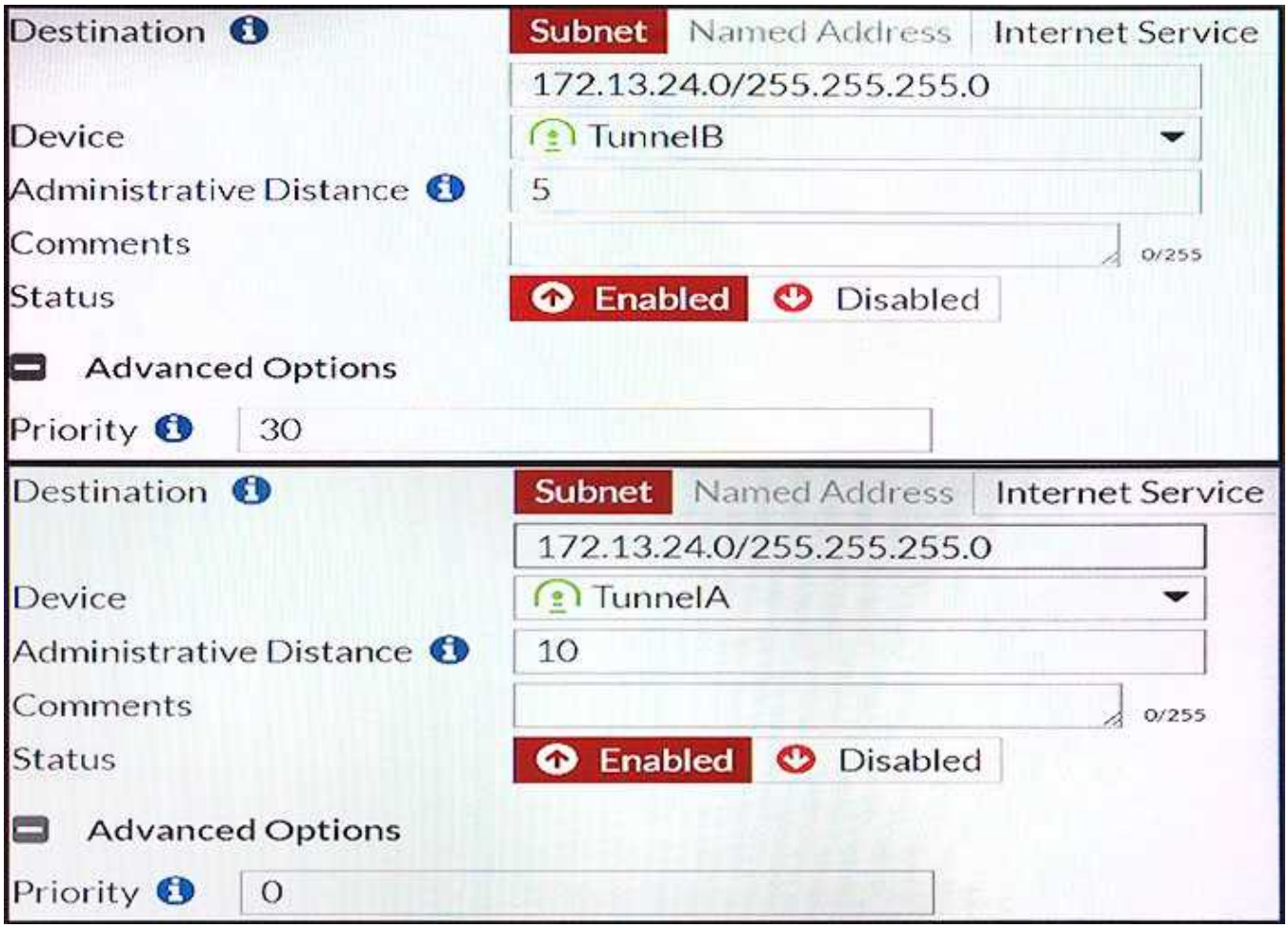
You are tasked to architect a new IPsec deployment with the following criteria:
- There are two HQ sites that all satellite offices must connect to.
- The satellite offices do not need to communicate directly with other satellite offices.
- No dynamic routing will be used.
- The design should minimize the number of tunnels being configured.
Which topology should be used to satisfy all of the requirements?

A. Redundant
B. Hub-and-spoke
C. Partial mesh
D. Fully meshed

Answer: B

Question: 6

View the exhibit.



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

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

Answer: A,B

Question: 7

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

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

Answer: C,D

Question: 8

An administrator needs to offload logging to FortiAnalyzer from a FortiGate with an internal hard drive. Which statements are true? (Choose two.)

A. Logs must be stored on FortiGate first, before transmitting to FortiAnalyzer
B. FortiGate uses port 8080 for log transmission
C. Log messages are transmitted as plain text in LZ4 compressed format (store-and-upload method).
D. FortiGate can encrypt communications using SSL encrypted OFTP traffic.

Answer: A,C

Question: 9

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

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

Answer: B,D

Question: 10

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

Answer: A,B,C

Question: 11

View the example routing table.

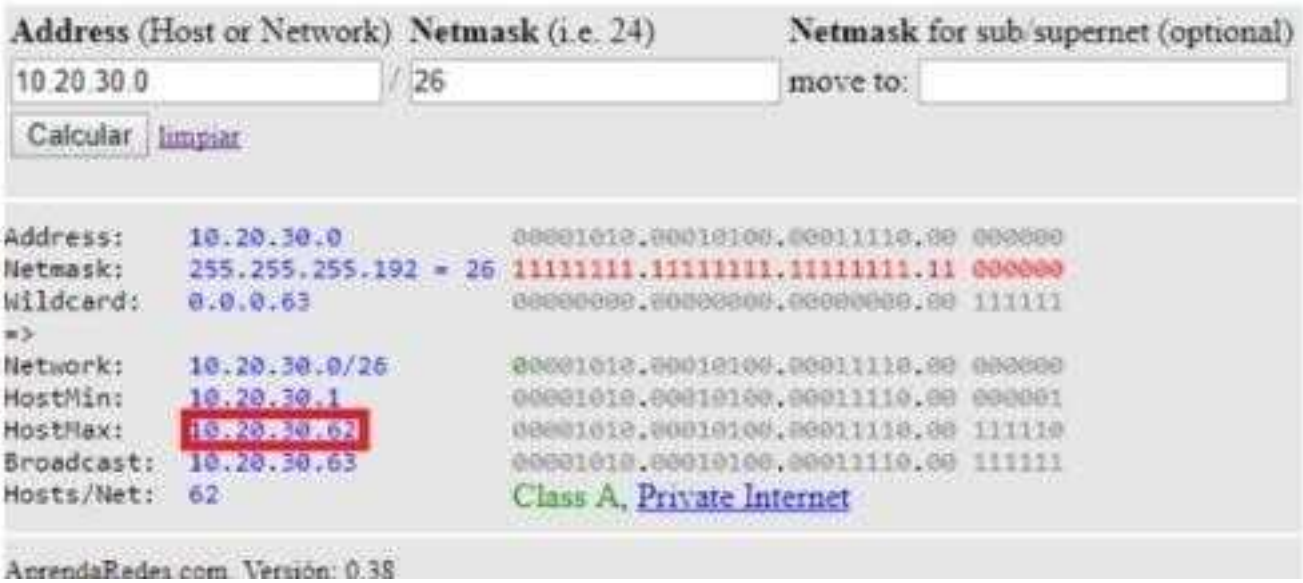
```
S*    0.0.0.0/0 [10/0] via 172.20.121.2, port1
C     172.20.121.0/24 is directly connected, port1
C     172.20.168.0/24 is directly connected, port2
C     172.20.167.0/24 is directly connected, port3
S     10.20.30.0/26 [10/0] via 172.20.168.254, port2
S     10.20.30.0/24 [10/0] via 172.20.167.254, port3
```

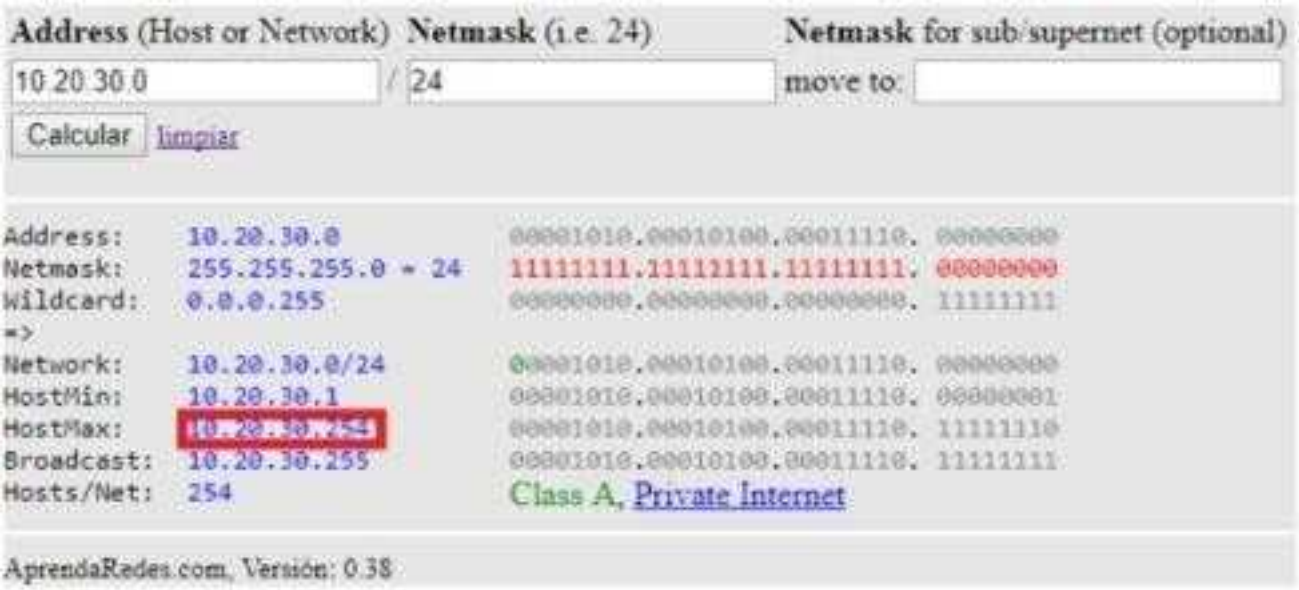
Which route will be selected when trying to reach 10.20.30.254?

A. 10.20.30.0/26 [10/0] via 172.20.168.254, port2
B. The traffic will be dropped because it cannot be routed.
C. 10.20.30.0/24 [10/0] via 172.20.167.254, port3
D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1

Answer: C

Explanation:





Question: 12

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

A. The FortiGate unit's public IP address
B. The FortiGate unit's internal IP address
C. The remote user's virtual IP address
D. The remote user's public IP address

Answer: B

Question: 13

What is FortiGate's behavior when local disk logging is disabled?

A. Only real-time logs appear on the FortiGate dashboard.
B. No logs are generated.
C. Alert emails are disabled.
D. Remote logging is automatically enabled.

Answer: A

Question: 14

What traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Traffic to inappropriate web sites
B. SQL injection attacks
C. Server information disclosure attacks

D. Credit card data leaks
E. Traffic to botnet command and control (C&C) servers

Answer: B,C,E

Question: 15

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

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

Answer: B,D

Question: 16

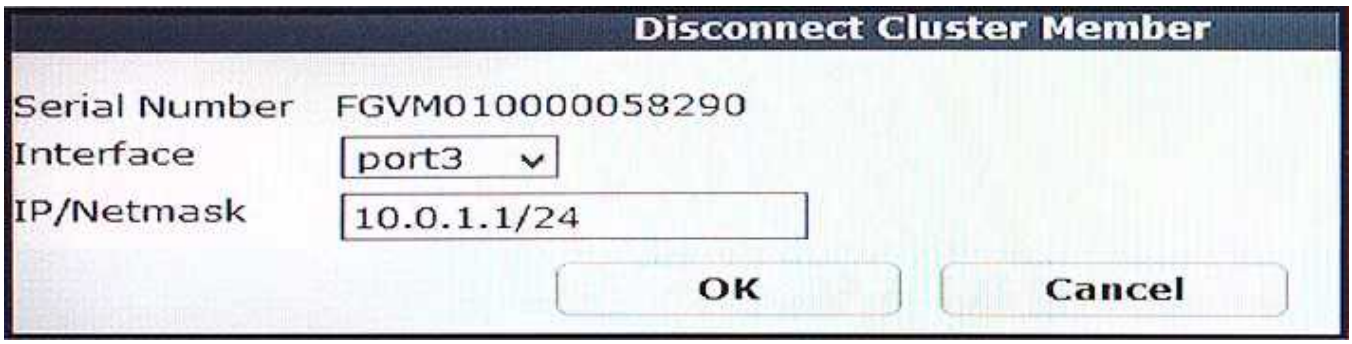
Which statements correctly describe transparent mode operation? (Choose three.)

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

Answer: C,D,E

Question: 17

View the exhibit.



What is the effect of the Disconnect Cluster Member operation as shown in the exhibit? (Choose two.)

A. The HA mode changes to standalone.
B. The firewall policies are deleted on the disconnected member.
C. The system hostname is set to the FortiGate serial number.

D. The port3 is configured with an IP address for management access.

Answer: A,D

Question: 18

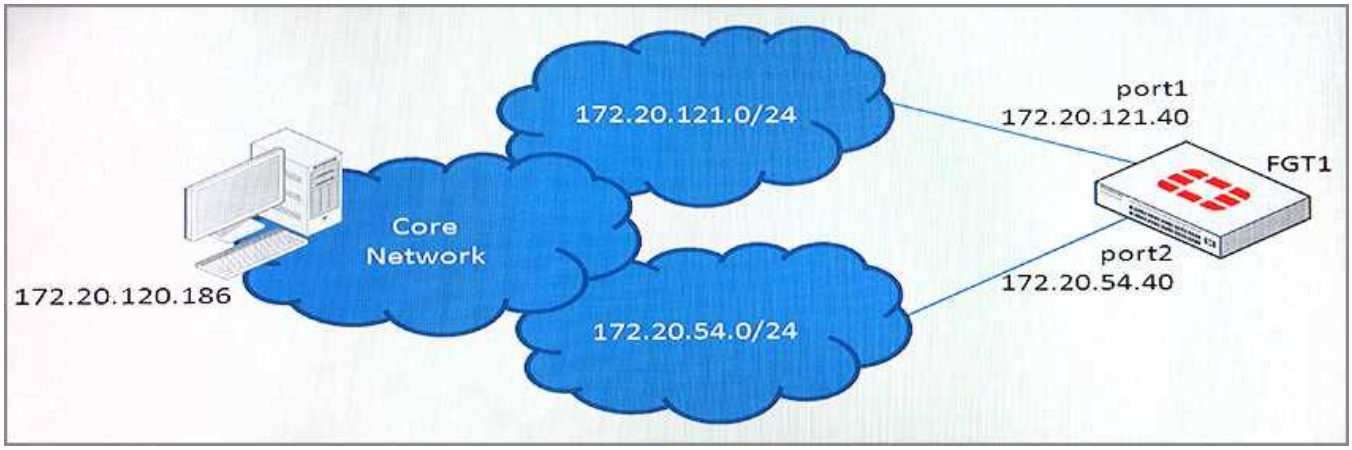
What step is required to configure an SSL VPN to access to an internal server using port forward mode?

A. Configure the virtual IP addresses to be assigned to the SSL VPN users.
B. Install FortiClient SSL VPN client
C. Create a SSL VPN realm reserved for clients using port forward mode.
D. Configure the client application to forward IP traffic to a Java applet proxy.

Answer: D

Question: 19

View the exhibit.



This is a sniffer output of a telnet connection request from 172.20.120.186 to the port1 interface of FGT1.

```
FGTI # di sniff pack any "host 172.20.120.186 and port 23" 4

4.571724 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
7.575327 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
9.571446 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
```

In this scenario. FGT1 has the following routing table:

```
S*    0.0.0.0/0 [10/0] via 172.20.54.254, port2
C     172.20.54.0/24 is directly connected, port2
C     172.20.121.0/24 is directly connected, port1
```

Assuming telnet service is enabled for port1, which of the following statements correctly describes

why FGT1 is not responding?

A. The port1 cable is disconnected.
B. The connection is dropped due to reverse path forwarding check.
C. The connection is denied due to forward policy check.
D. FGT1's port1 interface is administratively down.

Answer: B

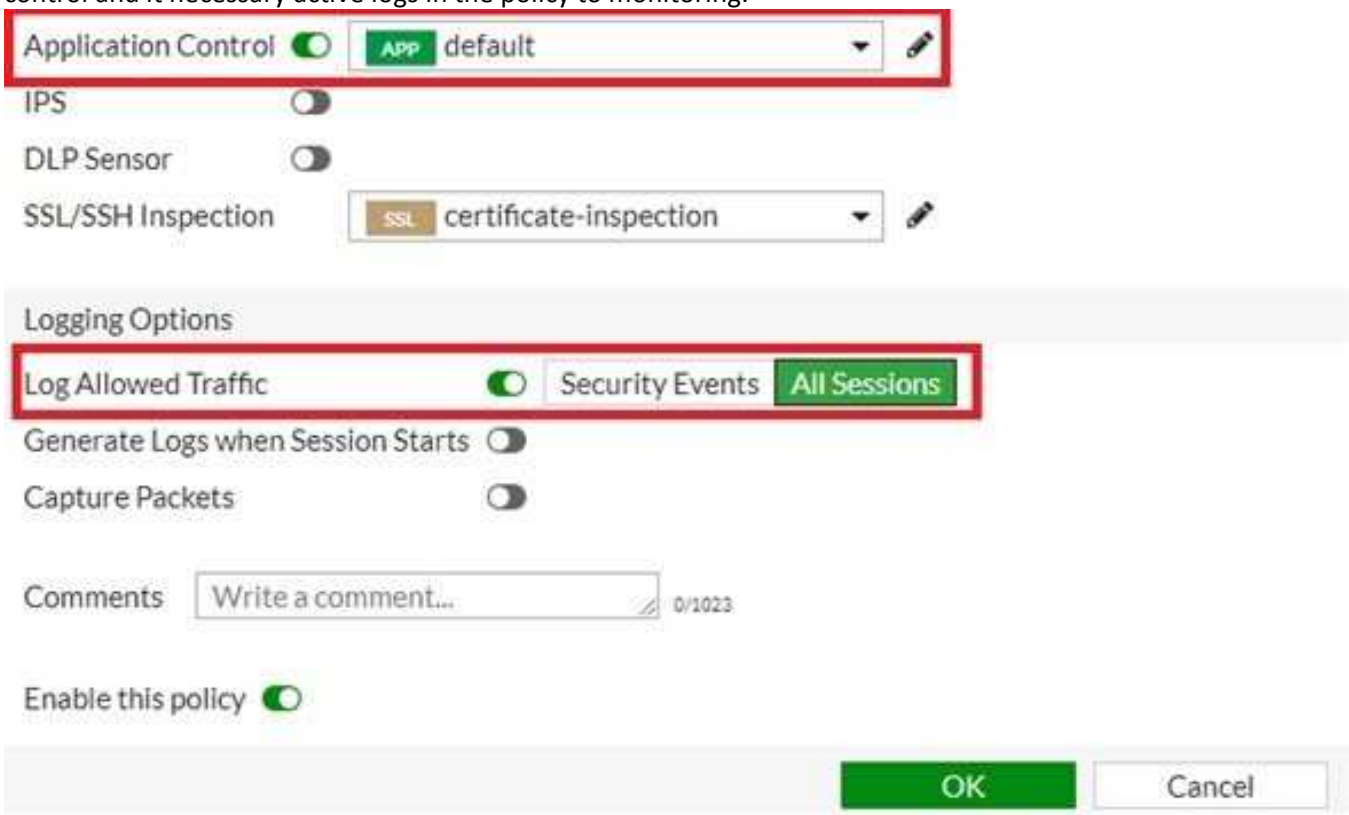
Question: 20

An administrator needs to be able to view logs for application usage on your network. What configurations are required to ensure that FortiGate generates logs for application usage activity? (Choose two.)

A. Enable a web filtering profile on the firewall policy.
B. Create an application control policy.
C. Enable logging on the firewall policy.
D. Enable an application control security profile on the firewall policy.

Answer: C,D

Explanation:
By default the fortigate have one app control to monitor and for that not need create other app control and it necessary active logs in the policy to monitoring.



Question: 21

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. Two separated SSL VPNs in different interfaces of the same VDOM
B. Different SSL VPN realms for each group
C. Different virtual SSLVPN IP addresses for each group
D. Two firewall policies with different captive portals

Answer: B

Explanation:

Question: 22

Examine the routing database.

```
S     *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
      *>           [10/0] via 10.0.0.2, port2, [30/0]
S        0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C     *> 10.0.0.0/24 is directly connected, port2
S        172.13.24.0/24 [10/0] is directly connected, port4
C     *> 172.20.121.0/24 is directly connected, port1
S     *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C     *> 192.168.15.0/24 is directly connected, port3
```

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

A. The port3 default route has the lowest metric, making it the best route.

B. There will be eight routes active in the routing table.
C. The port3 default has a higher distance than the port1 and port2 default routes.
D. Both port1 and port2 default routers are active in the routing table.

Answer: C,D

Question: 23

View the exhibit.

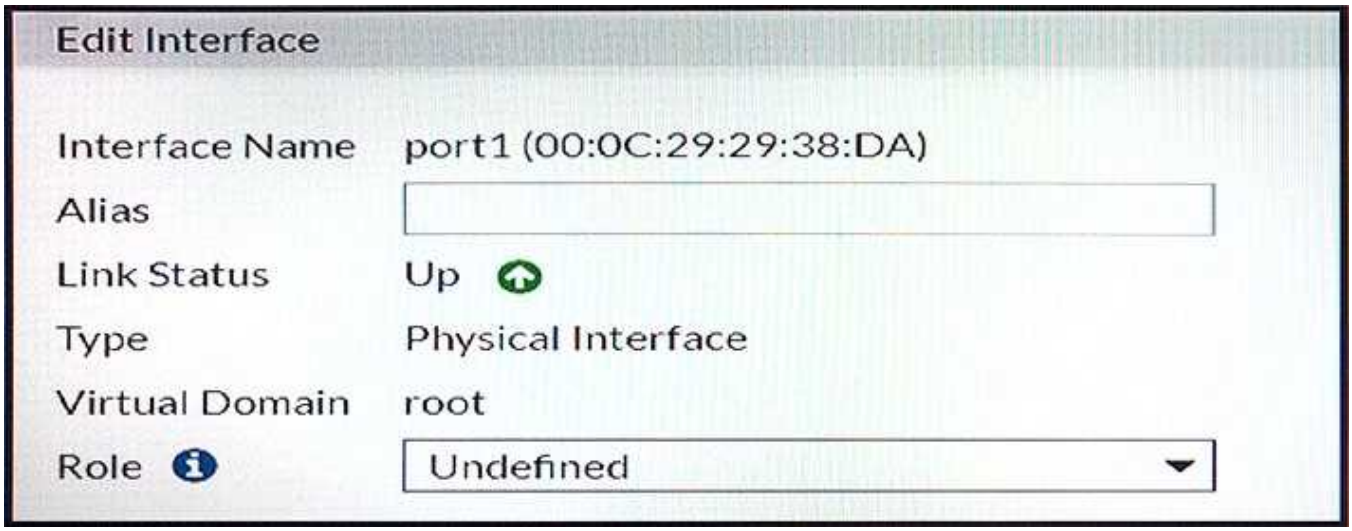
When a user attempts to connect to an HTTPS site, what is the expected result with this configuration?

A. The user is required to authenticate before accessing sites with untrusted SSL certificates.
B. The user is presented with certificate warnings when connecting to sites that have untrusted SSL certificates.
C. The user is allowed access all sites with untrusted SSL certificates, without certificate warnings.
D. The user is blocked from connecting to sites that have untrusted SSL certificates (no exception provided).

Answer: B

Question: 24

View the exhibit.



When Role is set to Undefined, which statement is true?

A. The GUI provides all the configuration options available for the port1 interface.
B. You cannot configure a static IP address for the port1 interface because it allows only DHCP addressing mode.
C. Firewall policies can be created from only the port1 interface to any interface.
D. The port1 interface is reserved for management only.

Answer: A

Question: 25

Which statement is true regarding the policy ID numbers of firewall policies?

A. Change when firewall policies are re-ordered.
B. Defines the order in which rules are processed.
C. Are required to modify a firewall policy from the CLI.
D. Represent the number of objects used in the firewall policy.

Answer: C

Explanation:
The ID no change when re-ordered and the rules are processed to top to bottom not by ID.

ID	Seq.#	Name	Source	Destination
port1 - port2 (1 - 2)				
2	1	VALID2	autoupdate.opera.com	all
1	2	VALID	Prueba	all

Question: 26

An administrator needs to inspect all web traffic (including Internet web traffic) coming from users connecting to SSL VPN. How can this be achieved?

A. Disabling split tunneling
B. Configuring web bookmarks
C. Assigning public IP addresses to SSL VPN clients
D. Using web-only mode

Answer: A

Explanation:

Question: 27

Which traffic inspection features can be executed by a security processor (SP)? (Choose three.)

A. TCP SYN proxy
B. SIP session helper
C. Proxy-based antivirus
D. Attack signature matching
E. Flow-based web filtering

Answer: C,D,E

Question: 28

An administrator has configured two VLAN interfaces:

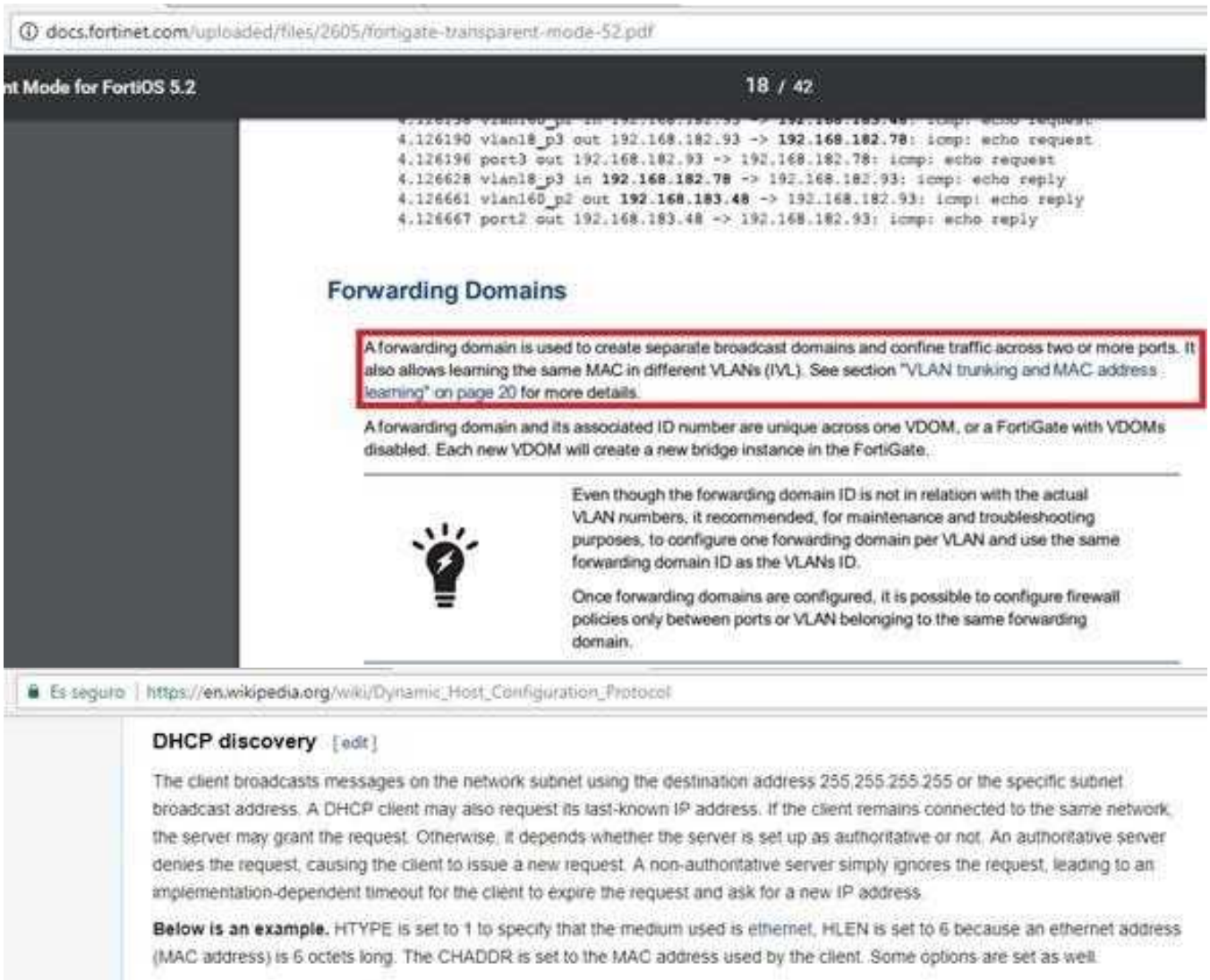
```
config system interface
     edit "VLAN10"
          set vdom "VDOM1"
          set forward-domain 100
          set role lan
          set interface "port9"
          set vlanid 10
     next
     edit "VLAN5"
          set vdom "VDOM1"
          set forward-domain 50
          set role lan
          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 be in different VDOMs
B. Both interfaces must have the same VLAN ID.
C. The role of the VLAN10 interface must be set to server.
D. Both interfaces must belong to the same forward domain.

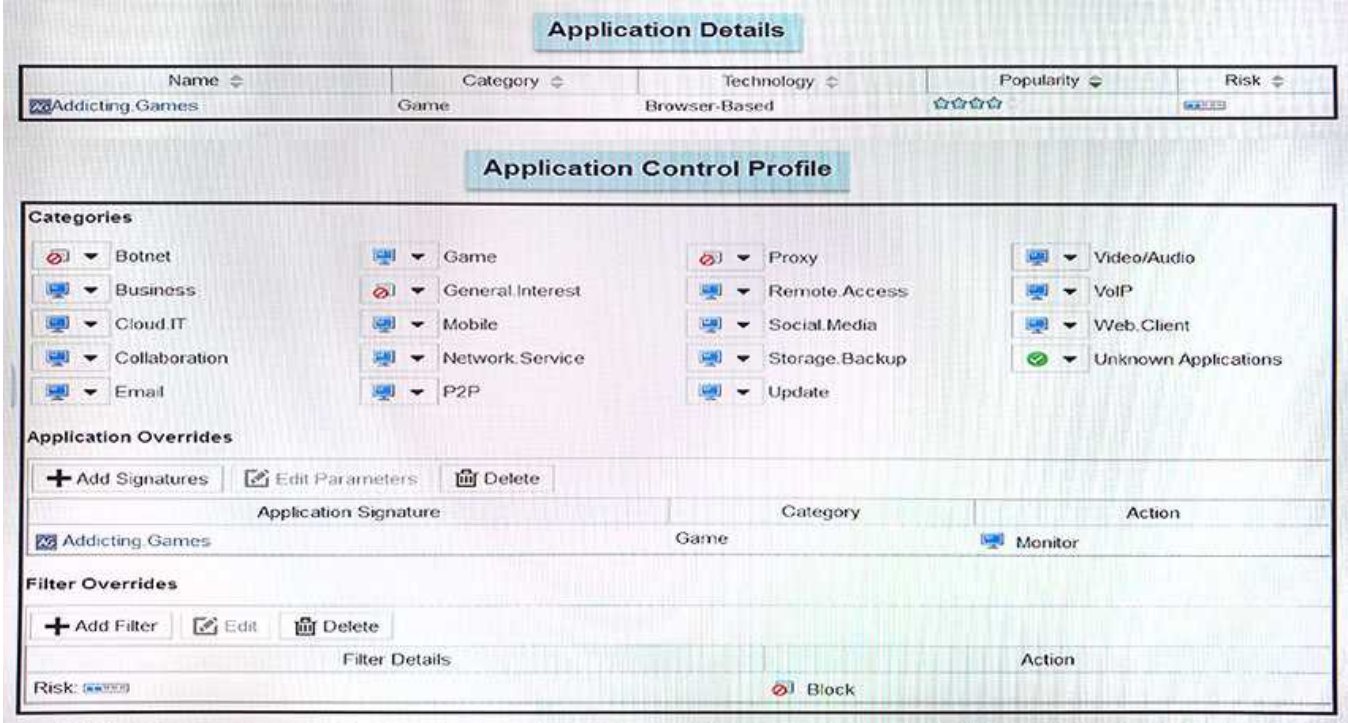
Answer: D

Explanation:



Question: 29

View the exhibit.



A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting.Games). Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.
B. Addicting.Games is blocked based on the Filter Overrides configuration.
C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
D. Addicting.Games is allowed based on the Categories configuration.

Answer: A

Question: 30

What are the purposes of NAT traversal in IPsec? (Choose two.)

A. To detect intermediary NAT devices in the tunnel path.
B. To encapsulate ESP packets in UDP packets using port 4500.
C. To force a new DH exchange with each phase 2 re-key
D. To dynamically change phase 1 negotiation mode to Aggressive.

Answer: A,B