QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

Fortinet

NSE4-5-4

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Question: 488

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: 489

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: 490

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: 491

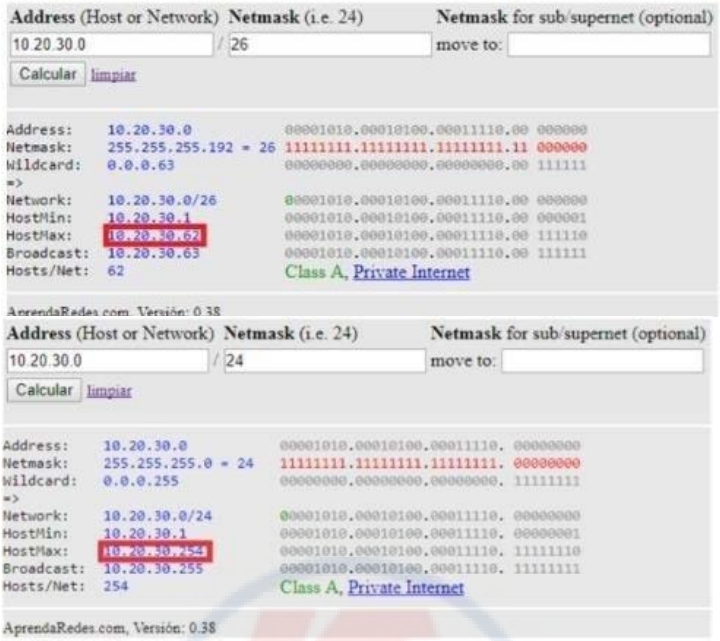
View the example routing table.

```
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: 492

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: 493

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: 494

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 SLAA,C 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: 495

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: 496

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: 497

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

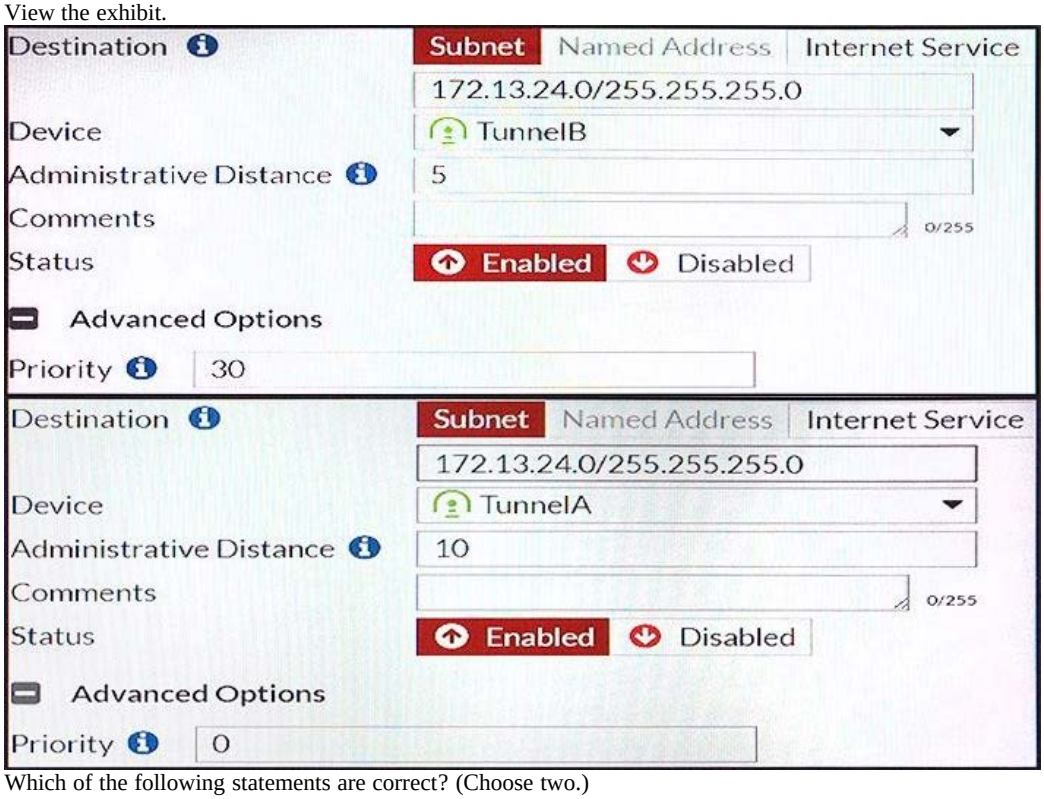
Question: 498

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: 499

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: 500

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