Fortinet

Exam Questions NSE4-5.4

Fortinet Network Security Expert - FortiOS 5.4

NEW QUESTION 1
Which action does the FortiGate take when link health monitor times out?

A. All routes to the destination subnet configured in the link health monitor are removed from the routing table.
B. The distance values of all routes using interface configured in the link health monitor are increased.
C. The priority values of all routes using configured in the link health monitor are increased.
D. All routes using the next-hop gateway configured in the link health monitor are removed from the routing table.

Answer: D

NEW QUESTION 2
Which of the following fields contained in the IP/TCP/UDP headers can be used to make a routing decision when using policy-based routing? (Choose three)

A. Source IP address.
B. TCP flags
C. Source TCP/UDP ports
D. Type of service.
E. Checksum

Answer: ACD

NEW QUESTION 3
The exhibit shoes three static routes.

```
config router static
    edit 1
      set dst 172.20.168.0 255.255.255.0
      set distance 10
      set priority 10
     set device port1
    next
    edit 2
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port2
    next
    edit 3
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port3
    next
end
```

Which routes will be used to route the packets to the destination IP address 172.20.168.1?

A. The route with the ID number 2 and 3.
B. Only the route with the ID number 3.
C. Only the route with the ID number 2.
D. Only the route with the ID number 1.

Answer: D

NEW QUESTION 4
The exhibit shows a FortiGate routing table. Which of the following statements are correct? (Choose two)

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
O*E2  0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C        172.16.78.0/24 is directly connected, wan2
O        192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30:28
C        192.168.3.0/24 is directly connected, dmz
C        192.168.11.0/24 is directly connected, internal
```

A. There is only one active default route.

B. The distance values for the route to 192.168.1.0/24 is 200
C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.
D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Answer: AD

NEW QUESTION 5
Which of the following statements are true regarding DLP File Type Filtering? (Choose two.)

A. Filters based on file extension
B. Filters based on fingerprints
C. Filters based on file content
D. File types are hard coded in the FortiOS

Answer: AC

Explanation:

NEW QUESTION 6
A network administrator needs to implement dynamic route redundancy between a FortiGate unit
located in a remote office and a FortiGate unit located in the central office.
The remote office accesses central resources using IPSec VPN tunnels through two different Internet providers.
What is the best method for allowing the remote office access to the resources through the FortiGate unit used at the central office?

A. Use two or more route-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
B. Use two or more policy-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.
C. Use route-based VPNs on the central office FortiGate unit to advertise routes with a dynamic routing protocol and use a policy-based VPN on the remote office with two or more static default routes.
D. Dynamic routing protocols cannot be used over IPSec VPN tunnels.

Answer: A

NEW QUESTION 7
An organization wishes to protect its SIP Server from call flooding attacks. Which of the following
configuration changes can be performed on the FortiGate unit to fulfill this requirement?

A. Apply an application control list which contains a rule for SIP and has the "Limit INVITE Request" option configured.
B. Enable Traffic Shaping for the appropriate SIP firewall policy.
C. Reduce the session time-to-live value for the SIP protocol by running the configure system session- ttl CLI command.
D. Run the set udp-idle-timer CLI command and set a lower time value.

Answer: A

NEW QUESTION 8
What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fully-
meshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a hub and spoke topology simplifies configuration.
C. Using a hub and spoke topology provides stronger encryption.
D. Using a hub and spoke topology reduces the number of tunnels.

Answer: BD

NEW QUESTION 9
Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The available actions for URL Filtering are Allow and Block.
B. Multiple URL Filter lists can be added to a single Web filter profile.
C. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.
D. The available actions for URL Filtering are Allow, Block and Exempt.

Answer: D

NEW QUESTION 10
A FortiGate unit can create a secure connection to a client using SSL VPN in tunnel mode. Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

A. Split tunneling can be enabled when using tunnel mode SSL VPN.
B. Software must be downloaded to the web client to be able to use a tunnel mode SSL VPN.
C. Users attempting to create a tunnel mode SSL VPN connection must be members of a configured user group on the FortiGate unit.
D. Tunnel mode SSL VPN requires the FortiClient software to be installed on the user's computer.
E. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Answer: ABCE

NEW QUESTION 11
A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received.
Which of the following statements are possible reasons for this? (Select all that apply.)

A. The external facing interface of the FortiGate unit is configured to use DHCP.
B. The FortiGate unit has not been registered.
C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network and no override push IP is configured.
D. The FortiGate unit is in Transparent mode which does not support push updates.

Answer: ABC

NEW QUESTION 12
Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

A. Proxy-based
B. DNS-based
C. Flow-based
D. Man-in-the-middle.

Answer: C

NEW QUESTION 13
An administrator has formed a high availability cluster involving two FortiGate units.
[Multiple upstream Layer 2 switches] -- [FortiGate HA Cluster] -- [Multiple downstream Layer 2 switches]
The administrator wishes to ensure that a single link failure will have minimal impact upon the overall throughput of traffic through this cluster.
Which of the following options describes the best step the administrator can take? The administrator should .

A. Increase the number of FortiGate units in the cluster and configure HA in active-active mode.
B. Enable monitoring of all active interfaces.
C. Set up a full-mesh design which uses redundant interfaces.
D. Configure the HA ping server feature to allow for HA failover in the event that a path is disrupted

Answer: C

NEW QUESTION 14
Regarding the header and body sections in raw log messages, which statement is correct?

A. The header and body section layouts change depending on the log type.
B. The header section layout is always the same regardless of the log typ
C. The body section layout changes depending on the log type.
D. Some log types include multiple body sections.
E. Some log types do not include a body section.

Answer: B

NEW QUESTION 15
What FortiGate feature can be used to block a ping sweep scan from an attacker?

A. Web application firewall (WAF)
B. Rate based IPS signatures

C. One-arm sniffer
D. DoS policies

Answer: B

NEW QUESTION 16
Which traffic sessions can be offloaded to a NP6 processor? (Choose two.)

A. IPv6
B. RIP
C. GRE
D. NAT64

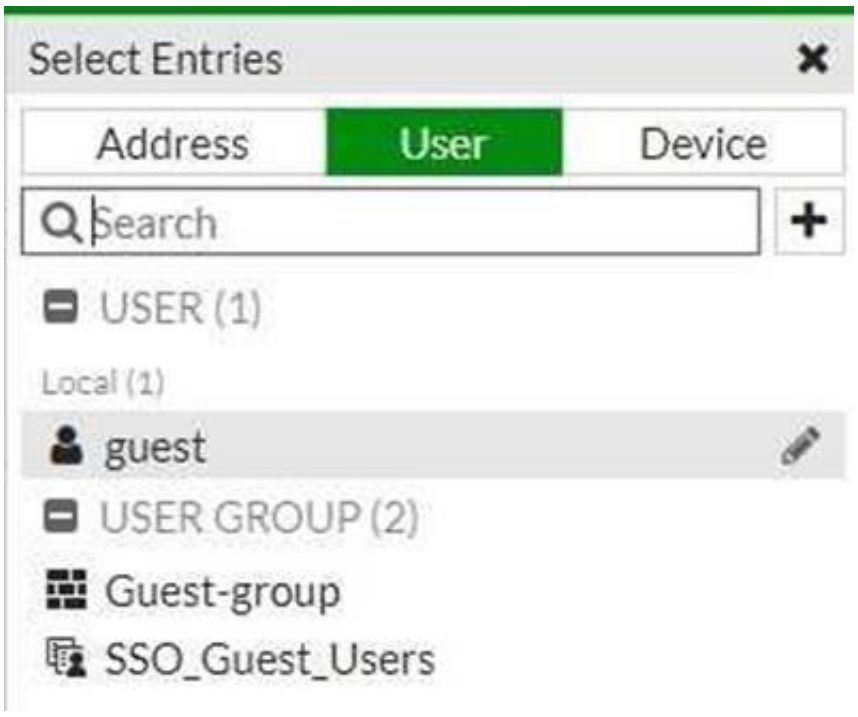
Answer: AD

NEW QUESTION 17
Which configuration objects can be selected for the Source filed of a firewall policy? (Choose two.)

A. FQDN address
B. IP pool
C. User or user group
D. Firewall service

Answer: AC

Explanation:



NEW QUESTION 18
Which statements about antivirus scanning using flow-based full scan are true? (Choose two.)

A. The antivirus engine starts scanning a file after the last packet arrives.
B. It does not support FortiSandbox inspection.
C. FortiGate can insert the block replacement page during the first connection attempt only if a virus is detected at the start of the TCP stream.
D. It uses the compact antivirus database.

Answer: AC

NEW QUESTION 19
Which of the following settings and protocols can be used to provide secure and restrictive administrative access to FortiGate? (Choose three.)

A. Trusted host
B. HTTPS
C. Trusted authentication
D. SSH
E. FortiTelemetry

Answer: ABD

NEW QUESTION 20
Which of the following statements best describes what a Certificate Signing Request (CSR) is?

A. A message sent by the Certificate Authority (CA) that contains a signed digital certificate.
B. An enquiry submitted to a Certificate Authority (CA) to request a root CA certificate
C. An enquiry submitted to a Certificate Authority (CA) to request a signed digital certificate
D. An enquiry submitted to a Certificate Authority (CA) to request a Certificate Revocation List (CRL)

Answer: B

NEW QUESTION 21
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE4-5.4 Practice Exam Features:

* NSE4-5.4 Questions and Answers Updated Frequently

* NSE4-5.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE4-5.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4-5.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year