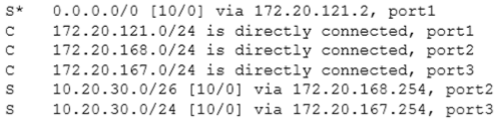
Fortinet NSE4-5.4 Exam

Volume: 89 Questions

Question: 1
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

Question: 2
When using WPAD DNS method, what is the FQDN format that browsers use to query the DNS server?

A. wpad.<local-domain>

B. srv_tcp.wpad.<local-domain>

C. srv_proxy.<local-domain>/wpad.dat

D. proxy.<local-domain>.wpad

Answer: A

Question: 3
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.

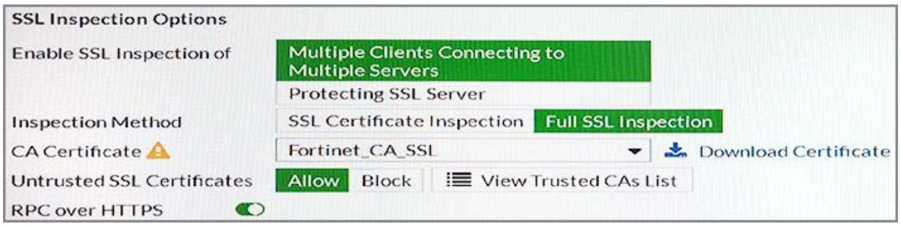
C. FortiGate can insert the block replacement page during the first connection attempt only if a virus is detected at the start of the TCP stream.

D. It uses the compact antivirus database.

Answer: A,C

Question: 4

View the exhibit.



SSL Inspection Options

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers | Protecting SSL Server

Inspection Method: SSL Certificate Inspection | Full SSL Inspection

CA Certificate: Fortinet_CA_SSL — Download Certificate

Untrusted SSL Certificates: Allow | Block — View Trusted CAs List

RPC over HTTPS

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.

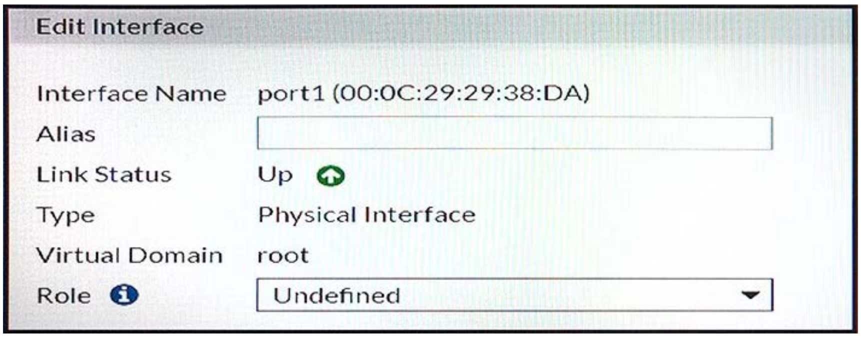
C. The user is allowed access all sites with untrusted SSL certificates, without certificate warnings.

D. The user is blocked from connecting to sites that have untrusted SSL certificates (no exception provided).

Answer: B

Question: 5

View the exhibit.



Edit Interface

Interface Name: port1 (00:0C:29:29:38:DA)

Alias:

Link Status: Up

Type: Physical Interface

Virtual Domain: root

Role: Undefined

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: 6
Which of the following statements about NTLM authentication are correct? (Choose two.)

A. It is useful when users log in to DCs that are not monitored by a collector agent.

B. It takes over as the primary authentication method when configured alongside FSSO.

C. Multi-domain environments require DC agents on every domain controller.

D. NTLM-enabled web browsers are required.

Answer: A,C

Question: 7
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.

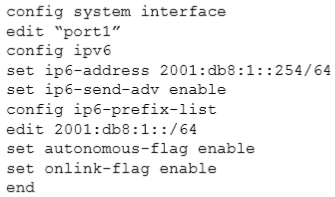
C. Enable logging on the firewall policy.

D. Enable an application control security profile on the firewall policy.

Answer: C,D

Question: 8

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: 9

Which statement about the firewall policy authentication timeout is true?

A. It is a hard timeout. The FortiGate removes the temporary policy for a user’s source IP address after this times expires.

B. It is a hard timeout. The FortiGate removes the temporary policy for a user’s source MAC address after this times expires.

C. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user’s source MAC address.

D. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user’s source IP.

Answer: D

Question: 10

Which configuration steps must be performed on both units to support this scenario? (Choose three.)

A. Define the phase 2 parameters.

B. Set the phase 2 encapsulation method to transport mode.

C. Define at least one firewall policy, with the action set to IPsec.

D. Define a route to the remote network over the IPsec tunnel.

E. Define the phase 1 parameters, without enabling IPsec interface mode.

Answer: A,D,E

Question: 11
How to configure Collector agent settings?

A. The dead entry timeout interval is used to age out entries with an unverified status.

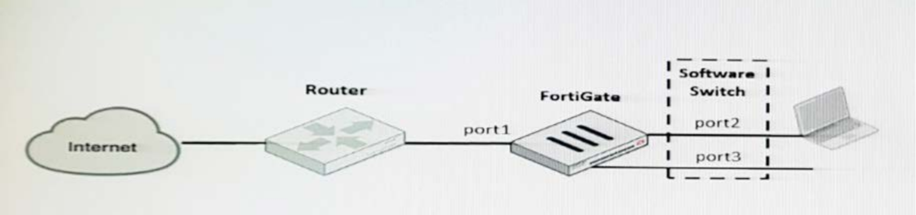
B. The workstation verify interval is used to periodically check if a workstation is still a domain member.

C. The user group cache expiry is used to age out the monitored groups.

D. The IP address change verify interval monitors the server IP address where the collector agent is installed, and updates the collector agent configuration if it changes.

Answer: D

Question: 12
A client workstation is connected to FortiGate port2. The Fortigate port1 is connected to an ISP router. Port2 and port3 are both configured as a software switch.



What IP address must be configured in the workstation as the default gateway?

A. The port2's IP address.

B. The router's IP address.

C. The FortiGate's management IP address.