Free Questions for NSE4_FGT-7.2 by certsdeals

Shared by Lloyd on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin ->sink: org pre->post, reply pre->post dev=5->3/3 ->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53 -> 10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

Options:

A- The session is a UDP unidirectional state.

B- The session is in TCP ESTABLISHED state.

C- The session is a bidirectional UDP connection.

D- The session is a bidirectional TCP connection.

Answer:

C

Explanation:

https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

Question 2

Question Type: MultipleChoice

Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides

(client and server) have terminated the session?

Options:

A- To remove the NAT operation.

B- To generate logs

C- To finish any inspection operations.

D- To allow for out-of-order packets that could arrive after the FIN/ACK packets.

Answer:

D

Question 3

Question Type: **MultipleChoice**

What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?

Options:

A- It limits the scanning of application traffic to the DNS protocol only.

B- It limits the scanning of application traffic to use parent signatures only.

C- It limits the scanning of application traffic to the browser-based technology category only.

D- It limits the scanning of application traffic to the application category only.

Answer:

C

Explanation:

FortiGate Security 7.2 Study Guide (p.317): 'You can configure the URL Category within the same security policy; however, adding a URL filter causes application control to scan applications in only the browser-based technology category, for example, Facebook Messenger on the Facebook website.'

Question 4

Question Type: MultipleChoice

Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

Options:

A- Shut down/reboot a downstream FortiGate device.

B- Disable FortiAnalyzer logging for a downstream FortiGate device.

C- Log in to a downstream FortiSwitch device.

D- Ban or unban compromised hosts.

Answer:

A, B

Question 5

Question Type: **MultipleChoice**

Examine the exhibit, which contains a virtual IP and firewall policy configuration.

Exhibit A | Exhibit B

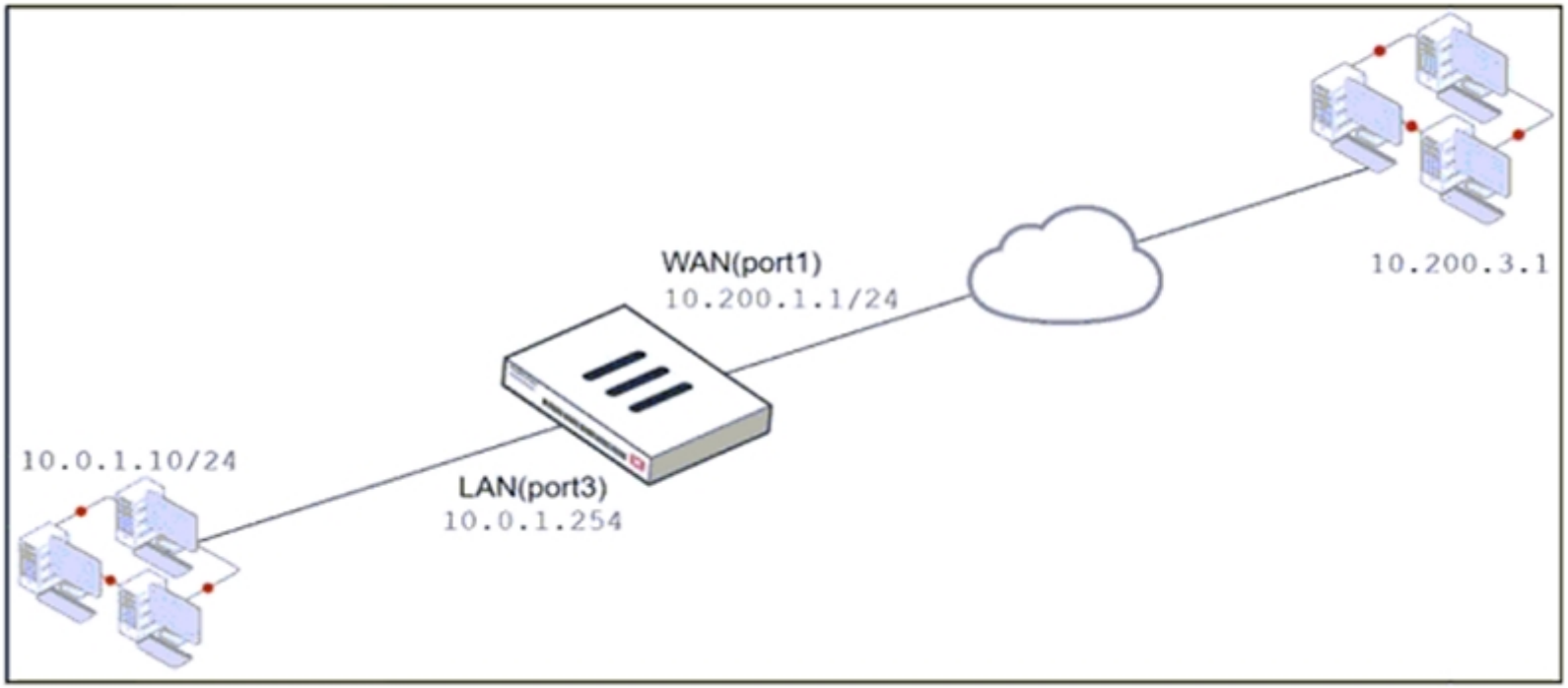


Exhibit A | Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type IPv4
Name VIP
Comments Write a comment... 0/255
Color Change

Network
Interface WAN (port1)
Type Static NAT
External IP address/range 10.200.1.10
Map to
IPv4 address/range 10.0.1.10

Optional Filters

Port Forwarding
Protocol TCP UDP SCTP ICMP
Port Mapping Type One to one Many to many
External service port 10443
Map to IPv4 port 443

The WAN (port1) interface has the IP address 10.200. 1. 1/24. The LAN (port2) interface has the IP address 10.0. 1.254/24.

The first firewall policy has NAT enabled on the outgoing interface address. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0. 1. 10/24?

Options:

A- 10.200. 1. 10

B- Any available IP address in the WAN (port1) subnet 10.200. 1.0/24

C- 10.200. 1. 1

D- 10.0. 1.254

Answer:

A

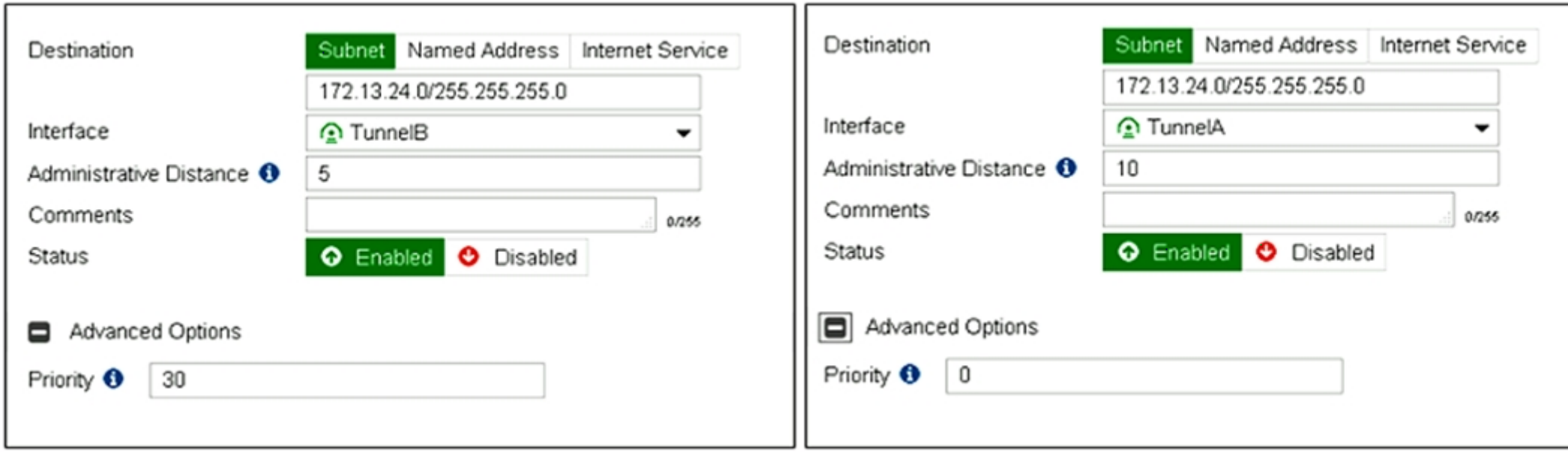
Explanation:

https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs.

Question 6

Question Type: MultipleChoice

View the exhibit.



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

Options:

A- This setup requires at least two firewall policies with the action set to IPsec.

B- Dead peer detection must be disabled to support this type of IPsec setup.

C- The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.

D- This is a redundant IPsec setup.

Answer:

C, D

Explanation:

https://docs.fortinet.com/document/fortigate/6.2.4/cookbook/632796/ospf-with-ipsec-vpn-for-network-redundancy

Question 7

Question Type: MultipleChoice

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on

which device?

Options:

A- FortiManager

B- Root FortiGate

C- FortiAnalyzer

D- Downstream FortiGate

Answer:

B

Question 8

Question Type: **MultipleChoice**

Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srci ntfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dumytracker.org/"
sentbyte=517 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

Options:

A- Traffic is blocked because Action is set to DENY in the firewall policy.

B- Traffic belongs to the root VDOM.

C- This is a security log.

D- Log severity is set to error on FortiGate.

Answer:

B, C

Question 9

Question Type: MultipleChoice

FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)

Options:

A- Antivirus scanning

B- File filter

C- DNS filter

D- Intrusion prevention

Answer:

A, D

Question 10

Question Type: MultipleChoice

Consider the topology:

Application on a Windows machine FGT--> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.

The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

Options:

A- Set the maximum session TTL value for the TELNET service object.

B- Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.

C- Create a new service object for TELNET and set the maximum session TTL.

D- Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer:

C, D