NSE4$^{\text{Q\&As}}$

Fortinet Network Security Expert 4 Written Exam (400)

Pass Fortinet NSE4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

Which statement is correct regarding virus scanning on a FortiGate unit?

A. Virus scanning is enabled by default.

B. Fortinet customer support enables virus scanning remotely for you.

C. Virus scanning must be enabled in a security profile, which must be applied to a firewall policy.

D. Enabling virus scanning in a UTM security profile enables virus scanning for all traffic flowing through the FortiGate device.

Correct Answer: C

QUESTION 2

Files reported as "suspicious" were subject to which Antivirus check"?

A. Grayware

B. Virus

C. Sandbox

D. Heuristic

Correct Answer: D

QUESTION 3

You have created a new administrator account, and assign it the prof_admin profile. Which is false about that account\\'s permissions?

A. It cannot upgrade or downgrade firmware.

B. It can create and assign administrator accounts to parts of its own VDOM.

C. It can reset forgotten passwords for other administrator accounts such as "admin".

D. It has a smaller permissions scope than accounts with the "super_admin" profile.

Correct Answer: A

QUESTION 4

What are examples of correct syntax for the session table diagnostics command? (Choose two.)

A. diagnose sys session filter clear

B. diagnose sys session src 10.0.1.254

C. diagnose sys session filter

D. diagnose sys session filter list dst.

Correct Answer: AC

QUESTION 5

Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

A. CHAP

B. MSCHAP2

C. PAP

D. FSSO

Correct Answer: D

QUESTION 6

In which process states is it impossible to interrupt/kill a process? (Choose two.)

A. S-Sleep

B. R-Running

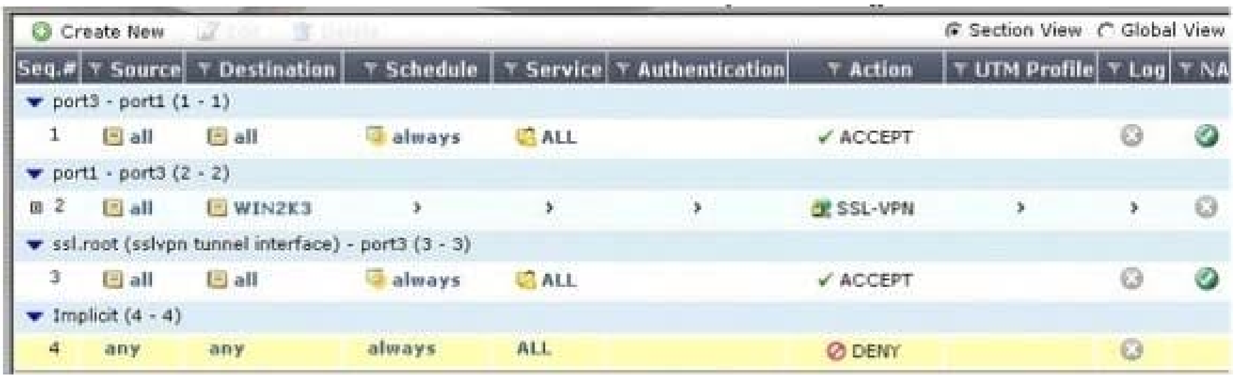
C. D-Uninterruptable Sleep

D. Z-Zombie

Correct Answer: CD

QUESTION 7

An end user logs into the full-access SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has enabled split tunneling.



Seq.#	Source	Destination	Schedule	Service	Authentication	Action	UTM Profile	Log	NA
port3 - port1 (1 - 1)									
1	all	all	always	ALL		✓ ACCEPT		⊗	✓
port1 - port3 (2 - 2)									
⊞ 2	all	WIN2K3	›	›	›	SSL-VPN	›	›	⊗
ssl.root (sslvpn tunnel interface) - port3 (3 - 3)									
3	all	all	always	ALL		✓ ACCEPT		⊗	✓
Implicit (4 - 4)									
4	any	any	always	ALL		⊘ DENY		⊗	

Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client\\'s routing table.

A. A route to destination matching the `WIN2K3\\' address object.

B. A route to the destination matching the `all\\' address object.

C. A default route.

D. No route is added.

Correct Answer: A

QUESTION 8

Which of the following are possible actions for static URL filtering? (Choose three.)

A. Allow

B. Block

C. Exempt

D. Warning

E. Shape

Correct Answer: ABC

QUESTION 9

What is valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

A. Users are required to manually enter their credentials each time they connect to a different web site.

B. Proxy users are authenticated via FSSO.

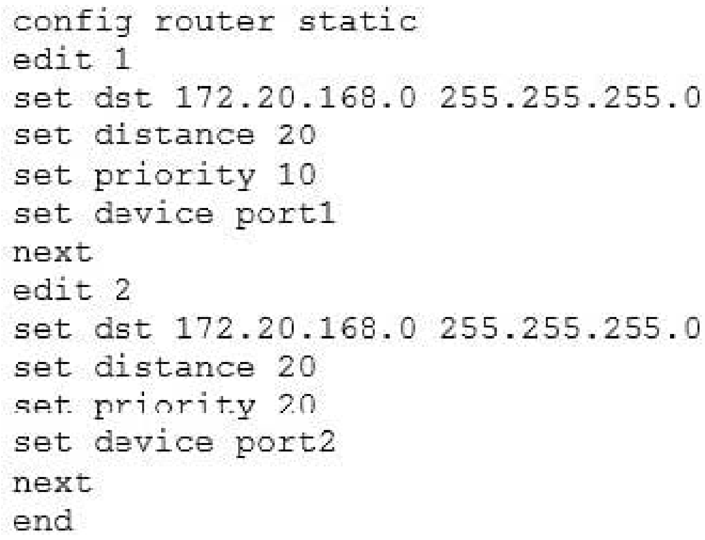
C. There are multiple users sharing the same IP address.

D. Proxy users are authenticated via RADIUS.

Correct Answer: C

QUESTION 10

Examine the two static routes to the same destination subnet 172.20.168.0/24 as shown below; then answer the question following it.



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

Which of the following statements correctly describes the static routing configuration provided above?

A. The FortiGate evenly shares the traffic to 172.20.168.0/24 through both routes.

B. The FortiGate shares the traffic to 172.20.168.0/24 through both routes, but the port2 route will carry approximately twice as much of the traffic.

C. The FortiGate sends all the traffic to 172.20.168.0/24 through port1.

D. Only the route that is using port1 will show up in the routing table.

Correct Answer: C

QUESTION 11

Examine this log entry.

What does the log indicate? (Choose three.)

date=2013-12-04 time=09:30:18 logid=0100032001 type=event subtype=system level=information vd="root" user="admin" ui=http(192.168.1.112) action=login status=success reason=none profile="super_admin" msg="Administrator admin logged in successfully from http(192.168.1.112)"

A. In the GUI, the log entry was located under "Log and Report > Event Log > User".

B. In the GUI, the log entry was located under "Log and Report > Event Log > System".

C. In the GUI, the log entry was located under "Log and Report > Traffic Log > Local Traffic".

D. The connection was encrypted.

E. The connection was unencrypted.

F. The IP of the FortiGate interface that "admin" connected to was 192.168.1.112.

G. The IP of the computer that "admin" connected from was 192.168.1.112.

Correct Answer: BEG

QUESTION 12

For traffic that does match any configured firewall policy, what is the default action taken by the FortiGate?

A. The traffic is allowed and no log is generated.

B. The traffic is allowed and logged.

C. The traffic is blocked and no log is generated.

D. The traffic is blocked and logged.

Correct Answer: C

QUESTION 13

Which of the following traffic shaping functions can be offloaded to a NP processor? (Choose two.)

A. Que prioritization

B. Traffic cap (bandwidth limit)

C. Differentiated services field rewriting

D. Guarantee bandwidth

Correct Answer: CD

QUESTION 14

Which of the following statements are characteristics of a FSSO solution using advanced access mode? (Choose three.)

A. Protection profiles can be applied to both individual users and user groups

B. Nested or inherited groups are supported

C. Usernames follow the LDAP convention: CN=User, OU=Name, DC=Domain

D. Usernames follow the Windows convention: Domain\username

E. Protection profiles can be applied to user groups only.

Correct Answer: BCE

QUESTION 15

A FortiGate device is configured with two VDOMs. The management VDOM is \\'root\\' , and is configured in transparent mode,\\'vdom1\\' is configured as NAT/route mode. Which traffic is generated only by \\'root\\' and not \\'vdom1\\'? (Choose three.)

A. SNMP traps

B. FortiGaurd

C. ARP

D. NTP

E. ICMP redirect

Correct Answer: ABD

NSE4 VCE Dumps NSE4 Study Guide NSE4 Braindumps