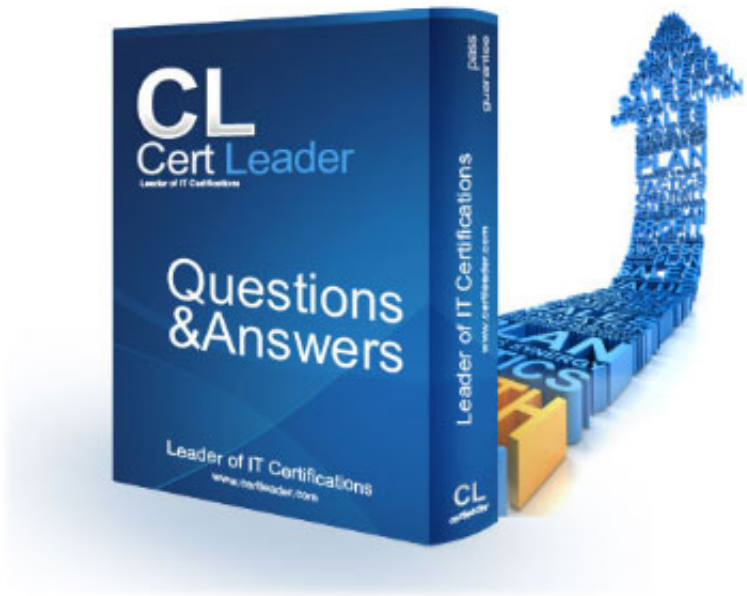
NSE4 - Fortinet Network Security Expert 4 Written Exam (400)

http://www.certleader.com/NSE4-dumps.html



1. 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.

Answer: C

2. A FortiGate unit operating in NAT/route mode and configured with two sub-interface on the same physical interface. Which of the following statement is correct regarding the VLAN IDs in this scenario?

A. The two VLAN sub-interfaces can have the same VLAN IDs only if they have IP addresses in different subnets.

B. The two VLAN sub-interfaces must have different VLAN IDs.

C. The two VLAN sub-interfaces can have VLAN ID only if they belong to different VDOMs.

D. The two VLAN sub-interfaces can have the same VLAN if they are connected to different L2 IEEE 802.1Q complaint switches.

Answer: B

3. What protocol cannot be used with the active authentication type?

A. Local

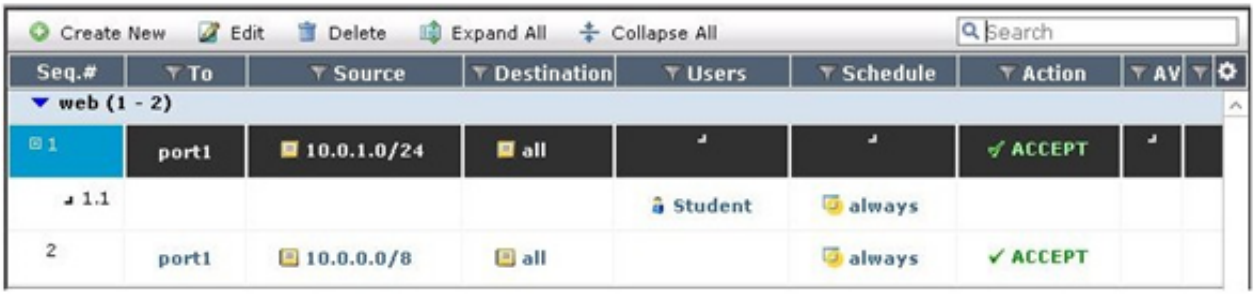
B. RADIUS

C. LDAP

D. RSSO

Answer: D

4. Review the exhibit of an explicit proxy policy configuration.



If there is a proxy connection attempt coming from the IP address 10.0.1.5, and from a user that has not authenticated yet, what action does the FortiGate proxy take?

A. User is prompted to authenticate. Traffic from the user Student will be allowed by the policy #1. Traffic from any other user will be allowed by the policy #2.

B. User is not prompted to authenticate. The connection is allowed by the proxy policy #2.

C. User is not prompted to authenticate. The connection will be allowed by the proxy policy #1.

D. User is prompted to authenticate. Only traffic from the user Student will be allowed. Traffic from any other user will be blocked.

Answer: D

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: B,C

6. How is traffic routed onto an SSL VPN tunnel from the FortiGate unit side?

A. A static route must be configured by the administrator using the ssl.root interface as the outgoing interface.

B. Assignment of an IP address to the client causes a host route to be added to the FortiGate unit's kernel routing table.

C. A route back to the SSLVPN IP pool is automatically created on the FortiGate unit.

D. The FortiGate unit adds a route based upon the destination address in the SSL VPN firewall policy.

Answer: B

7. Which of the following settings can be configured per VDOM? (Choose three)

A. Operating mode (NAT/route or transparent)

B. Static routes

C. Hostname

D. System time

E. Firewall Policies

Answer: A,B,E

8. Which protocols can you use for secure administrative access to a FortiGate? (Choose two)

A. SSH

B. Telnet

C. NTLM

D. HTTPS

Answer: A,D

9. A FortiGate administrator with the super_admin profile configures a virtual domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in the GUI in the management VDOM.

What would be a possible cause for this problem?

A. The administrator does not have the proper permissions the dmz interface.

B. The dmz interface is referenced in the configuration of another VDOM.

C. Non-management VDOMs cannot reference physical interfaces

D. The dmz interface is in PPPoE or DHCP mode.

Answer: B

10. Examine the exhibit; then answer the question below.

The Vancouver FortiGate initially had the following information in its routing table:

S 172.20.0.0/16 [10/0] via 172.21.1.2, port2

C 172.21.0.0/16 is directly connected, port2

C 172.11.11.0/24 is directly connected, port1

Afterwards, the following static route was added:

config router static edit 6

set dst 172.20.1.0 255.255.255.0

set priority 0

set device port1

set gateway 172.11.12.1 next

Since this change, the new static route is NOT showing up in the routing table. Given the information provided, which of the following describes the cause of this problem?

A. The subnet 172.20.1.0/24 is overlapped with the subnet of one static route that is already in the routing table (172.20.0.0/16), so, we need to enable allow-subnet-overlap first.

B. The 'gateway' IP address is NOT in the same subnet as the IP address of port1.

C. The priority is 0, which means that the route will remain inactive.

D. The static route configuration is missing the distance setting.

Answer: B

11. 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.

Answer: A,C

12. Your Linux email server runs on a non-standard port number, port 2525. Which statement is true?

A. IPS cannot scan that traffic for SMTP anomalies because of the non-standard port number. You must reconfigured the server to run on port 2.

B. To apply IPS to traffic to that server, you must configured FortiGate SMTP proxy to listen on port 2525

C. IPS will apply all SMTP signatures, regardless of whether they apply to clients or servers.

D. Protocol decoders automatically detect SMTP and scan for matches with appropriate IPS signature.

Answer: B

13. A new version of FortiOS firmware has just been released. When you upload new firmware, which is true?

A. If you upload the firmware image via the boot loader's menu from a TFTP server, it will not preserve the configuration. But if you upload new firmware via the GUI or CLI, as long as you are following a supported upgrade path, FortiOS will attempt to convert the existing configuration to be valid with any new or changed syntax.

B. No settings are preserved. You must completely reconfigure.

C. No settings are preserved. After the upgrade, you must upload a configuration backup file. FortiOS will ignore any commands that are not valid in the new OS. In those cases, you must reconfigure settings that are not compatible with the new firmware.

D. You must use FortiConverter to convert a backup configuration file into the syntax required by the new FortiOS, then upload it to FortiGate.

Answer: A

14. Which of the following FSSO agents are required for a DC agent mode solution? (Choose two.)

A. FSSO agent

B. DC agent

C. Collector agent

D. Radius server

Answer: B,C

15. 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.

Answer: C

16. Which statement best describes what the FortiGate hardware acceleration processors main

task is?

A. Offload traffic processing tasks from the main CPU.

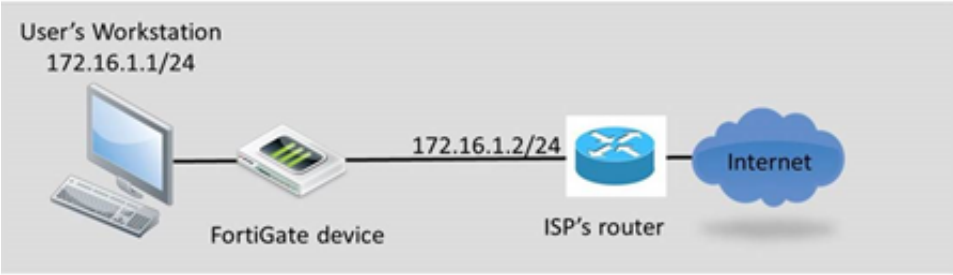
B. Offload management tasks from the main CPU.

C. Compress and optimize the network traffic.

D. Increase maximum bandwidth available in a FortiGate interface.

Answer: A

17. Review to the network topology in the exhibit.



The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet? (Choose two)

A. At least one firewall policy from port2 to port1 to allow outgoing traffic.

B. A default route configured in the FortiGuard devices pointing to the ISP's router.

C. Static or dynamic IP addresses in both ForitGate interfaces port1 and port2.

D. The FortiGate devices configured in transparent mode.

Answer: A,D

18. Which best describes the authentication timeout?

A. How long FortiGate waits for the user to enter his or her credentials.

B. How long a user is allowed to send and receive traffic before he or she must authenticate again.

C. How long an authenticated user can be idle (without sending traffic) before they must authenticate again.

D. How long a user-authenticated session can exist without having to authenticate again.

Answer: C

19. Which is NOT true about source matching with firewall policies?

A. A source address object must be selected in the firewall policy.

B. A source user/group may be selected in the firewall policy.

C. A source device may be defined in the firewall policy.

D. A source interface must be selected in the firewall policy.

E. A source user/group and device must be specified in the firewall policy.

Answer: E

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

A. Grayware

B. Virus

C. Sandbox

D. Heuristic

Answer: D

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4 Exam with Our Prep Materials Via below:

http://www.certleader.com/NSE4-dumps.html