

**NSE4 fortinet**

Number: NSE4  
Passing Score: 800  
Time Limit: 120 min



**Exam A****QUESTION 1**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 2**

Which antivirus and attack definition update options are supported by FortiGate units? (Choose two.)

- A. Manual update by downloading the signatures from the support site.
- B. FortiGuard pull updates.
- C. Push updates from a FortiAnalyzer.
- D. execute fortiguard-AV-AS command from the CLI.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 3**

Data leak prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Choose three.)

- A. POP3
- B. SNMP
- C. IPsec
- D. SMTP

E. HTTP

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 4

Which statements correctly describe transparent mode operation? (Choose three.)

- A. The FortiGate acts as transparent bridge and forwards traffic at Layer-2.
- B. Ethernet packets are forwarded based on destination MAC addresses, NOT IP addresses.
- C. The transparent FortiGate is clearly visible to network hosts in an IP trace route.
- D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.
- E. All interfaces of the transparent mode FortiGate device must be on different IP subnets.

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 5

Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic. What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

- A. They are offloaded to the NP6 in the master unit.
- B. They are not offloaded to the NP6 in the master unit.
- C. They are offloaded to the NP6 in the slave unit.
- D. They are not offloaded to the NP6 in the slave unit.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 6**

Which two methods are supported by the web proxy auto-discovery protocol (WPAD) to automatically learn the URL where a PAC file is located?  
(Choose two.)

- A. DHCP
- B. BOOTP
- C. DNS
- D. IPv6 autoconfiguration.

**Correct Answer:** AC

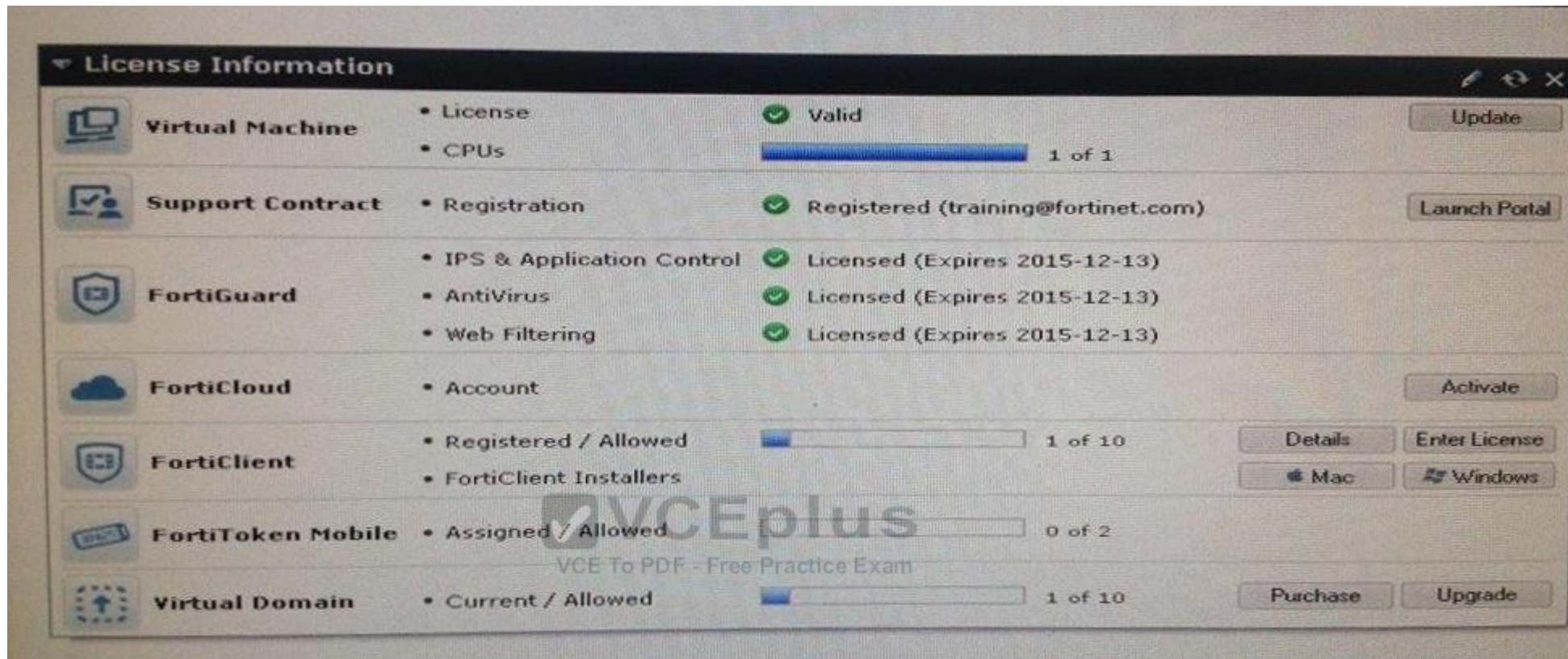
**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 7**

Examine the exhibit; then answer the question below.



Which statement describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

- A. They indicate that the FortiGate has the latest updates available from the FortiGuard Distribution Network.
- B. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
- C. They indicate that the FortiGate is in the process of downloading updates from the FortiGuard Distribution Network.
- D. They indicate that the FortiGate is able to connect to the FortiGuard Distribution Network.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 8**

Examine the static route configuration shown below; then answer the question following it.

```
config router static
  edit 1
    set dst 172.20.1.0 255.255.255.0
    set device port1
    set gateway 172.11.12.1
    set distance 10
    set weight 5
  next
  edit 2
    set dst 172.20.1.0 255.255.255.0
    set blackhole enable
    set distance 5
    set weight 10
  next
end
```

Which of the following statements correctly describes the static routing configuration provided? (Choose two.)

- A. All traffic to 172.20.1.0/24 is dropped by the FortiGate.
- B. As long as port1 is up, all traffic to 172.20.1.0/24 is routed by the static route number 1. if the interface port1 is down, the traffic is routed using the blackhole route.
- C. The FortiGate unit does NOT create a session entry in the session table when the traffic is being routed by the blackhole route.
- D. The FortiGate unit creates a session entry in the session table when the traffic is being routed by the blackhole route.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 9**

A user logs into a SSL VPN portal and activates the tunnel mode. The exhibit shows the firewall policy and the user's SSL VPN portal configuration:



Create New Edit Delete Section View Global View Search

Seq.#	Source	Destination	Schedule	Service	Action	NAT
port2 - port1 (1 - 1)						
1	all	all	always	ALL	✓ ACCEPT	✓ Enable
ssl.root (SSL VPN interface) - port2 (2 - 2)						
2	all training	Internal_Servers	always	ALL	✓ ACCEPT	✗ Disable
Implicit (3 - 3)						
3	all	all	always	ALL	✗ DENY	

Edit SSL-VPN Portal

Name full-access

☒ Enable Tunnel Mode

☒ Enable Split Tunneling

Routing Address Click to add...

Source IP Pools SSLVPN\_TUNNEL\_ADDR1 X

Client Options ☐ Save Password ☐ Auto Connect ☐ Always Up (Keep Alive)

Which static route is automatically added to the client's routing table when the tunnel mode is activated?

- A. A route to a destination subnet matching the *Internal\_Servers* address object.
- B. A route to the destination subnet configured in the tunnel mode widget.
- C. A default route.
- D. A route to the destination subnet configured in the SSL VPN global settings.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 10

Which header field can be used in a firewall policy for traffic matching?

- A. ICMP type and code.
- B. DSCP.
- C. TCP window size.
- D. TCP sequence number.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 11

A static route is configured for a FortiGate unit from the CLI using the following commands:

```
config router static
  edit 1
    set device "wan1"
    set distance 20
    set gateway 192.168.100.1
  next
end
```

Which of the following conditions are required for this static default route to be displayed in the FortiGate unit's routing table? (Choose two.)

- A. The administrative status of the wan1 interface is displayed as down.
- B. The link status of the wan1 interface is displayed as up.
- C. All other default routers should have a lower distance.
- D. The wan1 interface address and gateway address are on the same subnet.



**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 12

Which two statements are true regarding firewall policy disclaimers? (Choose two.)

- A. They cannot be used in combination with user authentication.
- B. They can only be applied to wireless interfaces.
- C. Users must accept the disclaimer to continue.
- D. The disclaimer page is customizable.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 13

In a high availability cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a slave unit?

- A. Client - > slave FortiGate - > master FortiGate - > web server.
- B. Client - > slave FortiGate - > web server.
- C. Client - > master FortiGate - > slave FortiGate - > master FortiGate - > web server.
- D. Client - > master FortiGate - > slave FortiGate - > web server.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 14

FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory. Which of the following statements are correct regarding FSSO in a Windows domain environment when DC-agent mode is used? (Choose two.)

- A. An FSSO collector agent must be installed on every domain controller.
- B. An FSSO domain controller agent must be installed on every domain controller.
- C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.
- D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 15

A FortiGate is configured with three virtual domains (VDOMs). Which of the following statements is correct regarding multiple VDOMs?

- A. The FortiGate must be a model 1000 or above to support multiple VDOMs.
- B. A license has to be purchased and applied to the FortiGate before VDOM mode could be enabled.
- C. Changing the operational mode of a VDOM requires a reboot of the FortiGate.
- D. The FortiGate supports any combination of VDOMs in NAT/Route and transparent modes.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 16

An administrator wants to create an IPsec VPN tunnel between two FortiGate devices.

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

- A. Create firewall policies to allow and control traffic between the source and destination IP addresses.
- B. Configure the appropriate user groups to allow users access to the tunnel.
- C. Set the operating mode to IPsec VPN mode.
- D. Define the phase 2 parameters.
- E. Define the Phase 1 parameters.

**Correct Answer:** ADE

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 17**

Which network protocols are supported for administrative access to a FortiGate unit? (Choose three.)

- A. SMTP
- B. WINS
- C. HTTP
- D. Telnet
- E. SSH

**Correct Answer:** CDE

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 18**

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

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 19**

What is the FortiGate password recovery process?

- A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.

- B. Log in through the console port using the "maintainer" account within several seconds of physically power cycling the FortiGate.
- C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
- D. Interrupt the boot sequence and restore a configuration file for which the password has been modified.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 20

Which two web filtering inspection modes inspect the full URL? (Choose two.)

- A. DNS-based
- B. Proxy-based
- C. Flow-based
- D. URL-based

**Correct Answer:** BC

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### QUESTION 21

Which of the following statements are correct about the HA command `diagnose sys ha reset-uptime`? (Choose two.)

- A. The device this command is executed on is likely to switch from master to slave status if `override` is disabled.
- B. The device this command executed on is likely to switch from master to slave status if `override` is enabled.
- C. The command has no impact on the HA algorithm.
- D. This commands resets the uptime variable used in the HA algorithm so it may cause a new master to become elected.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

Which statements are correct properties of a partial mesh VPN deployment. (Choose two.)

- A. VPN tunnels interconnect between every single location.
- B. VPN tunnels are not configured between every single location.
- C. Some location may be reachable via a hub location.
- D. It cannot contain redundant VPN tunnels.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

How do you configure a FortiGate to apply traffic shaping to P2P traffic, such as BitTorrent?

- A. Apply a traffic shaper to a BitTorrent entry in an application control list, which is then applied to a firewall policy.
- B. Enable the *shape* option in a firewall policy with *service* set to BitTorrent.
- C. Define a DLP rule to match against BitTorrent traffic and include the rule in a DLP sensor with traffic shaping enabled.
- D. Apply a traffic shaper to a protocol options profile.

**Correct Answer:** A

**Section:** (none)




**Explanation**



**Explanation/Reference:**

**QUESTION 24**

Review the IPS sensor filter configuration shown in the exhibit.

**Pattern Based Signatures and Filters**

 Create New  Edit  Delete

▼ Severity	▼ Target	▼ OS	▼ Action	▼ P
Critical	Server	Linux	 Block	

Based on the information in the exhibit, which statements are correct regarding the filter? (Choose two.)

- A. It does not log attacks targeting Linux servers.
- B. It matches all traffic to Linux servers.
- C. Its action will block traffic matching these signatures.
- D. It only takes affect when the sensor is applied to a policy.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 25

Two devices are in an HA cluster, the device hostnames are STUDENT and REMOTE. Exhibit A shows the command output of `diagnose sys session stat` for the STUDENT device. Exhibit B shows the command output of `diagnose sys session stat` for the REMOTE device.

Exhibit A:



```
STUDENT # diagnose sys session stat
Misc info:      session_count=166 setup_rate=68 exp_count=0 clash=0
                memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
    8 in ESTABLISHED state
    3 in SYN_SENT state
    1 in FIN_WAIT state
   139 in TIME_WAIT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
    syncqf=0 acceptqf=0 no-listener=2 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

STUDENT # _
```

Exhibit B:

```
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # diagnose sys session stat
misc info:      session_count=11 setup_rate=0 exp_count=0 clash=4
               memory_tension_drop=0 ephemeral=0/57344 removeable=0  ha_scan=0
delete=0, flush=0, dev_down=0/0
TCP sessions:
               2 in ESTABLISHED state
               1 in SYN_SENT state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000000
tcp reset stat:
               syncqf=0 acceptqf=0 no-listener=7 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0

REMOTE # _
```

Given the information provided in the exhibits, which of the following statements are correct? (Choose two.)

- A. STUDENT is likely to be the master device.
- B. Session-pickup is likely to be enabled.
- C. The cluster mode is active-passive.
- D. There is not enough information to determine the cluster mode.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 26

Which statements are correct regarding an IPv6 over IPv4 IPsec configuration? (Choose two.)

- A. The source quick mode selector must be an IPv4 address.
- B. The destination quick mode selector must be an IPv6 address.
- C. The *Local Gateway IP* must be an IPv4 address.
- D. The remote gateway IP must be an IPv6 address.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/2712/fortigate-ipv6-54.pdf>

#### **QUESTION 27**

Which is not a FortiGate feature?

- A. Database auditing
- B. Intrusion prevention
- C. Web filtering
- D. Application control

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 28**

When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

- A. FortiGate will still subject that person's traffic to firewall policies; it will not bypass them.
- B. FortiGate will drop the packets and not respond.
- C. FortiGate responds with a block message, indicating that it will not allow that person to log in.
- D. FortiGate responds only if the administrator uses a secure protocol. Otherwise, it does not respond

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 29**

A backup file begins with this line:

```
#config-version=FGVM64-5.02-FW-build589-140613:opmode=0:vdom=0:user=admin #conf_file_ver=3881503152630288414 #buildno=0589  
#global_vdom=1
```

Can you restore it to a FortiWiFi 60D?

- A. Yes
- B. Yes, but only if you replace the "#conf\_file\_ver" line so that it contains the serial number of that specific FortiWiFi 60D.
- C. Yes, but only if it is running the same version of FortiOS, or a newer compatible version.
- D. No

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 30**

Acme Web Hosting is replacing one of their firewalls with a FortiGate. It must be able to apply port forwarding to their back-end web servers while blocking virus uploads and TCP SYN floods from attackers. Which operation mode is the best choice for these requirements?

- A. NAT/route
- B. NAT mode with an interface in one-arm sniffer mode
- C. Transparent mode
- D. No appropriate operation mode exists

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 31**

You have configured the DHCP server on a FortiGate's port1 interface (or internal, depending on the model) to offer IPs in a range of 192.168.1.65-

192.168.1.253.

When the first host sends a DHCP request, what IP will the DHCP offer?

- A. 192.168.1.99
- B. 192.168.1.253
- C. 192.168.1.65
- D. 192.168.1.66

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 32

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 33

Which UTM feature sends a UDP query to FortiGuard servers each time FortiGate scans a packet (unless the response is locally cached)?

- A. Antivirus
- B. VPN
- C. IPS
- D. Web Filtering

**Correct Answer:** D

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

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.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



**QUESTION 35**

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

- A. SSH
- B. Telnet
- C. NTLM
- D. HTTPS

**Correct Answer: AD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 36**

If you have lost your password for the "admin" account on your FortiGate, how should you reset it?



- A. Log in with another administrator account that has "super\_admin" profile permissions, then reset the password for the "admin" account.
- B. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to format the flash disk and reinstall the firmware. Then you can log in with the default password.
- C. Power off the FortiGate. After several seconds, restart it. Via the local console, within 30 seconds after booting has completed, log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.
- D. Reboot the FortiGate. Via the local console, during the boot loader, use the menu to log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 37**

What are the ways FortiGate can monitor logs? (Choose three.)

- A. MIB
- B. SMS
- C. Alert Emails
- D. SNMP
- E. FortiAnalyzer
- F. Alert Message Console



**Correct Answer:** CDF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 38**

To which remote device can the FortiGate send logs? (Choose three.)

- A. Syslog
- B. FortiAnalyzer
- C. Hard drive
- D. Memory

E. FortiCloud

**Correct Answer:** ABE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 39

In a Crash log, what does a status of 0 indicate?

- A. Abnormal termination of a process
- B. A process closed for any reason
- C. Scanunitd process crashed
- D. Normal shutdown with no abnormalities
- E. DHCP process crashed

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 40

There are eight (8) log severity levels that indicate the importance of an event. Not including Debug, which is only needed to log diagnostic data, what are both the lowest AND highest severity levels?

- A. Notification, Emergency
- B. Information, Critical
- C. Error, Critical
- D. Information, Emergency
- E. Information, Alert

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 41**

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 & Report > Event Log > User".
- B. In the GUI, the log entry was located under "Log & Report > Event Log > System".
- C. In the GUI, the log entry was located under "Log & 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

**Section:** (none)

**Explanation**



**Explanation/Reference:**

**QUESTION 42**

Where are most of the security events logged?

- A. Security log
- B. Forward Traffic log
- C. Event log
- D. Alert log
- E. Alert Monitoring Console

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 43**

What determines whether a log message is generated or not?

- A. Firewall policy setting
- B. Log Settings in the GUI
- C. 'config log' command in the CLI
- D. Syslog
- E. Webtrends

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 44**

Which of the following are considered log types? (Choose three.)

- A. Forward log
- B. Traffic log
- C. Syslog
- D. Event log
- E. Security log

**Correct Answer:** BDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 45**

What attributes are always included in a log header? (Choose three.)

- A. policyid
- B. level
- C. user
- D. time

- E. subtype
- F. duration

**Correct Answer:** BDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 46**

What log type would indicate whether a VPN is going up or down?

- A. Event log
- B. Security log
- C. Forward log
- D. Syslog

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 47**

Which correctly define "Section View" and "Global View" for firewall policies? (Choose two.)

- A. Section View lists firewall policies primarily by their interface pairs.
- B. Section View lists firewall policies primarily by their sequence number.
- C. Global View lists firewall policies primarily by their interface pairs.
- D. Global View lists firewall policies primarily by their policy sequence number.
- E. The 'any' interface may be used with Section View.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 48**

In "diag debug flow" output, you see the message "Allowed by Policy-1: SNAT". Which is true?

- A. The packet matched the topmost policy in the list of firewall policies.
- B. The packet matched the firewall policy whose policy ID is 1.
- C. The packet matched a firewall policy, which allows the packet and skips UTM checks
- D. The policy allowed the packet and applied session NAT.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 49**

Which is NOT true about the settings for an IP pool type port block allocation?

- A. A Block Size defines the number of connections.
- B. Blocks Per User defines the number of connection blocks for each user.
- C. An Internal IP Range defines the IP addresses permitted to use the pool.
- D. An External IP Range defines the IP addresses in the pool.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 50**

Which define device identification? (Choose two.)

- A. Device identification is enabled by default on all interfaces.
- B. Enabling a source device in a firewall policy enables device identification on the source interfaces of that policy.
- C. You cannot combine source user and source device in the same firewall policy.
- D. FortiClient can be used as an agent based device identification technique.
- E. Only agentless device identification techniques are supported.



**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 51

Which is true of FortiGate's session table?

- A. NAT/PAT is shown in the central NAT table, not the session table.
- B. It shows TCP connection states.
- C. It shows IP, SSL, and HTTP sessions.
- D. It does not show UDP or ICMP connection state codes, because those protocols are connectionless.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 52

Which is true about incoming and outgoing interfaces in firewall policies?

- A. A physical interface may not be used.
- B. A zone may not be used.
- C. Multiple interfaces may not be used for both incoming and outgoing.
- D. Source and destination interfaces are mandatory.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 53

For FortiGate devices equipped with Network Processor (NP) chips, which are true? (Choose three.)

- A. For each new IP session, the first packet always goes to the CPU.

- B. The kernel does not need to program the NPU. When the NPU sees the traffic, it determines by itself whether it can process the traffic
- C. Once offloaded, unless there are errors, the NP forwards all subsequent packets. The CPU does not process them.
- D. When the last packet is sent or received, such as a TCP FIN or TCP RST signal, the NP returns this session to the CPU for tear down.
- E. Sessions for policies that have a security profile enabled can be NP offloaded.

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 54

Which traffic can match a firewall policy's "Services" setting? (Choose three.)

- A. HTTP
- B. SSL
- C. DNS
- D. RSS
- E. HTTPS



**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 55

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.

**Correct Answer:** E

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 56**

If you enable the option "Generate Logs when Session Starts", what effect does this have on the number of traffic log messages generated for each session?

- A. No traffic log message is generated.
- B. One traffic log message is generated.
- C. Two traffic log messages are generated.
- D. A log message is only generated if there is a security event.

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 57**

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.

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 58**

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

- A. CHAP

- B. MSCHAP2
- C. PAP
- D. FSSO

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 59**

Which are valid replies from a RADIUS server to an ACCESS-REQUEST packet from a FortiGate? (Choose two.)

- A. ACCESS-CHALLENGE
- B. ACCESS-RESTRICT
- C. ACCESS-PENDING
- D. ACCESS-REJECT

**Correct Answer:** AD

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### **QUESTION 60**

What protocol cannot be used with the active authentication type?

- A. Local
- B. RADIUS
- C. LDAP
- D. RSSO

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 61**

When configuring LDAP on the FortiGate as a remote database for users, what is not a part of the configuration?

- A. The name of the attribute that identifies each user (Common Name Identifier).
- B. The user account or group element names (user DN).
- C. The server secret to allow for remote queries (Primary server secret).
- D. The credentials for an LDAP administrator (password).

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 62**

Which authentication methods does FortiGate support for firewall authentication? (Choose two.)

- A. Remote Authentication Dial in User Service (RADIUS)
- B. Lightweight Directory Access Protocol (LDAP)
- C. Local Password Authentication
- D. POP3
- E. Remote Password Authentication



**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 63**

Which methods can FortiGate use to send a One Time Password (OTP) to Two-Factor Authentication users? (Choose three.)

- A. Hardware FortiToken
- B. Web Portal
- C. Email
- D. USB Token
- E. Software FortiToken (FortiToken mobile)

**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 64**

Which user group types does FortiGate support for firewall authentication? (Choose three.)

- A. RSSO
- B. Firewall
- C. LDAP
- D. NTLM
- E. FSSO

**Correct Answer:** ABE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 65**

Which does FortiToken use as input when generating a token code? (Choose two.)

- A. User password
- B. Time
- C. User name
- D. Seed

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Explanation:**

The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device. The token password changes at regular time intervals, and the FortiAuthenticator unit is able to validate the entered passcode using the time and the secret seed information for that token.



Reference: <http://docs.fortinet.com/uploaded/files/2030/FortiAuthenticator-3.1-Admin-Guide.pdf>

#### QUESTION 66

What is not true of configuring disclaimers on the FortiGate?

- A. Disclaimers can be used in conjunction with captive portal.
- B. Disclaimers appear before users authenticate.
- C. Disclaimers can be bypassed through security exemption lists.
- D. Disclaimers must be accepted in order to continue to the authentication login or originally intended destination.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 67

Which statement best describes what SSL.root is?

- A. The name of the virtual network adapter required in each user's PC for SSL VPN Tunnel mode.
- B. The name of a virtual interface in the root VDOM where all the SSL VPN user traffic comes from.
- C. A Firewall Address object that contains the IP addresses assigned to SSL VPN users.
- D. The virtual interface in the root VDOM that the remote SSL VPN tunnels connect to.

**Correct Answer: B**




**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 68

A FortiGate is configured with the 1.1.1.1/24 address on the wan2 interface and HTTPS Administrative Access, using the default tcp port, is enabled for that interface. Given the SSL VPN settings in the exhibit.

Listen on Interface(s)	<input type="text" value="wan2"/>  
<i>This is generally your external interface (i.e. wan1)</i>	
Listen on Port	<input type="text" value="443"/> 

URL Path	Virtual Host	Max Concurrent U
Training		0
students		0

Which of the following SSL VPN login portal URLs are valid? (Choose two.)

- A. http://1.1.1.1:443/Training
- B. https://1.1.1.1:443/STUDENTS
- C. https://1.1.1.1/login
- D. https://1.1.1.1/

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 69

Which of the following statements are correct regarding SSL VPN Web-only mode? (Choose two.)

- A. It can only be used to connect to web services.

- B. IP traffic is encapsulated over HTTPS.
- C. Access to internal network resources is possible from the SSL VPN portal.
- D. The standalone FortiClient SSL VPN client CANNOT be used to establish a Web-only SSL VPN.
- E. It is not possible to connect to SSH servers through the VPN.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 70

Which of the following authentication methods can be used for SSL VPN authentication? (Choose three.)

- A. Remote Password Authentication (RADIUS, LDAP)
- B. Two-Factor Authentication
- C. Local Password Authentication
- D. FSSO
- E. RSSO

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 71

Which statement best describes what SSL VPN Client Integrity Check does?

- A. Blocks SSL VPN connection attempts from users that has been blacklisted.
- B. Detects the Windows client security applications running in the SSL VPN client's PCs.
- C. Validates the SSL VPN user credential.
- D. Verifies which SSL VPN portal must be presented to each SSL VPN user.
- E. Verifies that the latest SSL VPN client is installed in the client's PC.

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 72**

Which statement is not correct regarding SSL VPN Tunnel mode?

- A. IP traffic is encapsulated over HTTPS.
- B. The standalone FortiClient SSL VPN client can be used to establish a Tunnel mode SSL VPN.
- C. A limited amount of IP applications are supported.
- D. The FortiGate device will dynamically assign an IP address to the SSL VPN network adapter.

**Correct Answer: C**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 73**

What action does an IPsec Gateway take with the user traffic routed to an IPsec VPN when it does not match any phase 2 quick mode selector?

- A. Traffic is dropped
- B. Traffic is routed across the default phase 2.
- C. Traffic is routed to the next available route in the routing table.
- D. Traffic is routed unencrypted to the interface where the IPsec VPN is terminating.

**Correct Answer: A**

**Section: (none)**

**Explanation****Explanation/Reference:****QUESTION 74**

Which of the following authentication methods are supported in an IPsec phase 1? (Choose two.)

- A. Asymmetric Keys
- B. CA root digital certificates

- C. RSA signature
- D. Pre-shared keys

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 75

Which of the following IPsec configuration modes can be used for implementing L2TP-over-IPSec VPNs?

- A. Policy-based IPsec only.
- B. Route-based IPsec only.
- C. Both policy-based and route-based VPN.
- D. L2TP-over-IPSec is not supported by FortiGate devices.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 76

Which of the following IPsec configuration modes can be used when the FortiGate is running in NAT mode?

- A. Policy-based VPN only
- B. Both policy-based and route-based VPN.
- C. Route-based VPN only.
- D. IPSec VPNs are not supported when the FortiGate is running in NAT mode.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 77**

Which of the following statements is true regarding the differences between route-based and policy-based IPsec VPNs? (Choose two.)

- A. The firewall policies for policy-based are bidirectional. The firewall policies for route-based are unidirectional.
- B. In policy-based VPNs the traffic crossing the tunnel must be routed to the virtual IPsec interface. In route-based, it does not.
- C. The action for firewall policies for route-based VPNs may be Accept or Deny, for policy-based VPNs it is Encrypt.
- D. Policy-based VPN uses an IPsec interface, route-based does not.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 78**

Which portion of the configuration does an administrator specify the type of IPsec configuration (either policy-based or route-based)?

- A. Under the IPsec VPN global settings.
- B. Under the phase 2 settings.
- C. Under the phase 1 settings.
- D. Under the firewall policy settings.



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 79**

Which of the following options best defines what Diffie-Hellman is?

- A. A symmetric encryption algorithm.
- B. A "key-agreement" protocol.
- C. A "Security-association-agreement" protocol.
- D. An authentication algorithm.

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 80**

How many packets are interchanged between both IPSec ends during the negotiation of a main-mode phase 1?

- A. 5
- B. 3
- C. 2
- D. 6

**Correct Answer:** D

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 81**

Which of the following IKE modes is the one used during the IPsec phase 2 negotiation?

- A. Aggressive mode
- B. Quick mode
- C. Main mode
- D. Fast mode

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 82**

Which of the following statements are true about IPsec VPNs? (Choose three.)

- A. IPsec increases overhead and bandwidth.
- B. IPsec operates at the layer 2 of the OSI model.

- C. End-user's network applications must be properly pre-configured to send traffic across the IPsec VPN.
- D. IPsec protects upper layer protocols.
- E. IPsec operates at the layer 3 of the OSI model.

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 83

Which of the following statements is true regarding the TCP SYN packets that go from a client, through an implicit web proxy (transparent proxy), to a web server listening at TCP port 80? (Choose three.)

- A. The source IP address matches the client IP address.
- B. The source IP address matches the proxy IP address.
- C. The destination IP address matches the proxy IP address.
- D. The destination IP address matches the server IP addresses.
- E. The destination TCP port number is 80.

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 84

Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

- A. More than one proxy is supported.
- B. Can contain a list of destinations that will be exempt from the use of any proxy.
- C. Can contain a list of URLs that will be exempted from the FortiGate web filtering inspection.
- D. Can contain a list of users that will be exempted from the use of any proxy.

**Correct Answer:** BC

**Section:** (none)

**Explanation**



**Explanation/Reference:****QUESTION 85**

An Internet browser is using the WPAD DNS method to discover the PAC file's URL. The DNS server replies to the browser's request with the IP address 10.100.1.10. Which URL will the browser use to download the PAC file?

- A. http://10.100.1.10/proxy.pac
- B. https://10.100.1.10/
- C. http://10.100.1.10/wpad.dat
- D. https://10.100.1.10/proxy.pac

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 86**

Which of the following are benefits of using web caching? (Choose three.)

- A. Decrease bandwidth utilization
- B. Reduce server load
- C. Reduce FortiGate CPU usage
- D. Reduce FortiGate memory usage
- E. Decrease traffic delay

**Correct Answer:** ABE

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 87**

Review the exhibit of an explicit proxy policy configuration.

<div> <span>Create New</span> <span>Edit</span> <span>Delete</span> <span>Expand All</span> <span>Collapse All</span> <div>Search</div> </div>								
Seq.#	To	Source	Destination	Users	Schedule	Action	AV	
▼ web (1 - 2)								
1	port1	10.0.1.0/24	all			✓ ACCEPT		
1.1				Student	always			
2	port1	10.0.0.0/8	all		always	✓ ACCEPT		

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.

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 88

Which protocol can an Internet browser use to download the PAC file with the web proxy configuration?

- A. HTTPS
- B. FTP
- C. TFTP
- D. HTTP

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 89**

Which are the three different types of Conserve Mode that can occur on a FortiGate device? (Choose three.)

- A. Proxy
- B. Operating system
- C. Kernel
- D. System
- E. Device

**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 90**

What is longest length of time allowed on a FortiGate device for the virus scan to complete?

- A. 20 seconds
- B. 30 seconds
- C. 45 seconds
- D. 10 seconds

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 91**

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

- A. Grayware
- B. Virus
- C. Sandbox

D. Heuristic

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 92**

Which type of conserve mode writes a log message immediately, rather than when the device exits conserve mode?

A. Kernel

B. Proxy

C. System

D. Device

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 93**

Files that are larger than the oversized limit are subjected to which Antivirus check?

A. Grayware

B. Virus

C. Sandbox

D. Heuristic

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 94**

A FortiGate device is configure to perform an AV & IPS scheduled update every hour.

Virus Definitions

```
-----  
Version: 21.00487  
Contract Expiry Date: Tue Apr 29 00:00:00 2014  
Last Updated using scheduled update on Mon Jan  
20 01:05:33 2014  
Last Update Attempt: Mon Jan 20 10:08:56 2014  
Result: Updates Installed
```

```
FG100D3G12800939 # exe time  
current time is: 10:35:35  
last ntp sync: Mon Jan 20 09:51:59 2014
```

Given the information in the exhibit, when will the next update happen?

- A. 01:00
- B. 02:05
- C. 11:00
- D. 11:08

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

What is the maximum number of different virus databases a FortiGate can have?

- A. 5
- B. 2

- C. 3
- D. 4

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 96**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 97**

Which of the following statements are true regarding the web filtering modes? (Choose two.)

- A. Proxy based mode allows for customizable block pages to display when sites are prevented.
- B. Proxy based mode requires more resources than flow-based.
- C. Flow based mode offers more settings under the advanced configuration section of the GUI.
- D. Proxy based mode offers higher throughput than flow-based mode.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 98**

Which of the following web filtering modes can inspect the full URL? (Choose two.)

- A. Proxy based
- B. DNS based
- C. Policy based
- D. Flow based

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 99**

Examine the following log message attributes and select two correct statements from the list below. (Choose two.)

hostname=www.youtube.com profiletype="Webfilter\_Profile" profile="default" status="passthrough" msg="URL belongs to a category with warnings enabled"

- A. The traffic was blocked.
- B. The user failed authentication.
- C. The category action was set to warning.
- D. The website was allowed

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 100**

Which of the following are possible actions for FortiGuard web category filtering? (Choose three.)

- A. Allow
- B. Block
- C. Exempt

- D. Warning
- E. Shape

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 101

Which of the following actions can be used with the FortiGuard quota feature? (Choose three.)

- A. Allow
- B. Block
- C. Monitor
- D. Warning
- E. Authenticate

**Correct Answer:** CDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 102

Which of the following statements are true regarding application control? (Choose two.)

- A. Application control is based on TCP destination port numbers.
- B. Application control is proxy based.
- C. Encrypted traffic can be identified by application control.
- D. Traffic shaping can be applied to the detected application traffic.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 103

The exhibit is a screen shot of an Application Control profile.

**Categories**

- Botnet
- Business
- Cloud.IT
- Collaboration
- Email
- Game
- General.Interest
- Network.Service
- P2P
- Proxy
- Remote.Access
- Social.Media
- Storage.Backup
- Update
- Video/Audio
- VoIP
- Industrial
- Web.Others
- All Other Known Applications
- All Other Unknown Applications

**Application Overrides**

Application Signature	Category	Action
YouTube	Video/Audio	Monitor
YouTube_Video.Access	Video/Audio	Monitor
YouTube_Video.Play	Video/Audio	Monitor

**Options**

- ON Deep Inspection of Cloud Applications
- ON Allow and Log DNS Traffic
- ON Replacement Messages for HTTP-based Applications

Different settings are circled and numbered. Select the number identifying the setting which will provide additional information about YouTube access, such as the name of the video watched.

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 104**

How do application control signatures update on a FortiGate device?

- A. Through FortiGuard updates.
- B. Upgrade the FortiOS firmware to a newer release.
- C. By running the Application Control auto-learning feature.
- D. Signatures are hard coded to the device and cannot be updated.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 105**

Which answer best describes what an "Unknown Application" is?

- A. All traffic that matches the internal signature for unknown applications.
- B. Traffic that does not match the RFC pattern for its protocol.
- C. Any traffic that does not match an application control signature
- D. A packet that fails the CRC check.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 106**

What actions are possible with Application Control? (Choose three.)

- A. Warn
- B. Allow
- C. Block

- D. Traffic Shaping
- E. Quarantine

**Correct Answer:** BCD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 107

Which of the following statements are true regarding application control? (choose two)

- A. Application control is based on TCP destination port numbers.
- B. Application control is proxy based.
- C. Encrypted traffic can be identified by application control.
- D. Traffic Shaping can be applied to the detected application traffic.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### QUESTION 108

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

**Correct Answer:** ACD

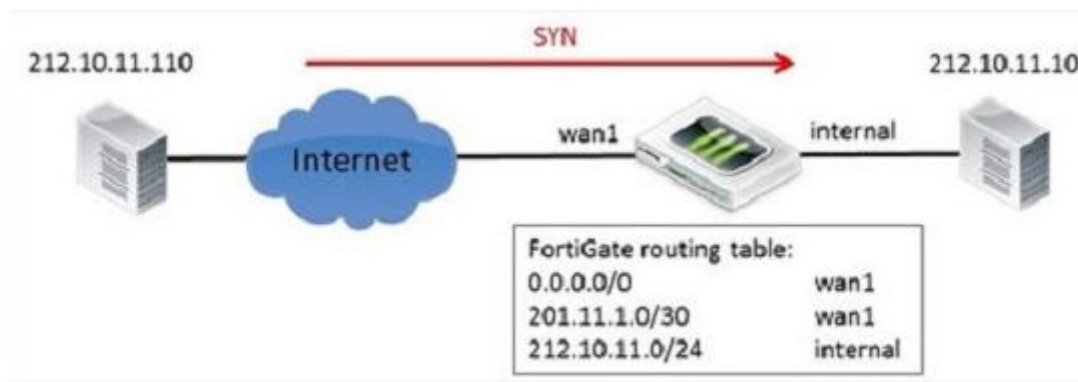
**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 109

Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



Which of the following sentences best describes the result of the reverse path forwarding (RPF) check executed by the FortiGate on the SYN packets? (Choose two).

- A. Packets is allowed if RPF is configured as loose.
- B. Packets is allowed if RPF is configured as strict.
- C. Packets is blocked if RPF is configured as loose.
- D. Packets is blocked if RPF is configured as strict.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 110

Which of the following statements best describe what a FortiGate does when packets match a black hole route?

- A. Packets are dropped.
- B. Packets are routed based on the information in the policy-based routing table.

- C. An ICMP error message is sent back to the originator.
- D. Packet are routed back to the originator.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 111

The exhibit shows two static routes to the same destinations subnet 172.20.168.0/24.

```
#config router static
edit 1
  set dst 172.20.168.0 255.255.255.0
  set distance 10
  set priority 20
  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 this static routing configuration? (choose two)

- A. Both routes will show up in the routing table.
- B. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 between routes.
- C. Only one route will show up in the routing table.
- D. The FortiGate will route the traffic to 172.20.168.0/24 only through one route.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 112**

Which of the following statements are true regarding WAN Link Load Balancing? (Choose two).

- A. There can be only one virtual WAN Link per VDOM.
- B. FortiGate can measure the quality of each link based on latency, jitter, or packets percentage.
- C. Link health checks can be performed over each link member if the virtual WAN interface.
- D. Distance and priority values are configured in each link member if the virtual WAN interface.


**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 113**

In the debug command output shown in the exhibit, which of the following best described the MAC address 00:09:0f:69:03:7e ?

  
VCE To PDF - Free Practice Exam  

```
# diagnose ip arp list
index=2 ifname=port1 172.20.187.150 00:09:0f:69:03:7e
state=00000004 use=4589 confirm=4589 update=2422 ref=1
```

- A. It is one of the secondary MAC addresses of the port1 interface.
- B. It is the primary MAC address of the port interface.
- C. It is the MAC address of another network devices located in the same LAN segment as the FortiGate unit's port1 interface.
- D. It is the HA virtual MAC address.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 114**

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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 115**

What must be configured in order to keep two static routes to the same destination in the routing table?

- A. The same priority.
- B. The same distance and same priority.
- C. The same distance.
- D. The same metric.



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 116**

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.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 117**

The exhibit shows a FortiGate routing table.

```
# 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
```

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

- 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

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 118**

A FortiGate device has two VDOMs in NAT/route mode. Which of the following solutions can be implemented by a network administrator to route traffic between the two VDOMs.(Choose two)

- A. Use the inter-VDOMs links automatically created between all VDOMS.
- B. Manually create and configured an inter-VDOM link between yours.
- C. Interconnect and configure an external physical interface in one VDOM to another physical interface in the second VDOM.
- D. Configure both VDOMs to share the same table.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 119**

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. FortiGuard
- C. ARP
- D. NTP
- E. ICMP redirect



**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 120**

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

**Correct Answer:** ABE

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 121**

Which of the following statements are correct regarding FortiGate virtual domains (VDMs)? (Choose two)

- A. VDMs divide a single FortiGate unit into two or more independent firewall.
- B. A management VDM handles SNMP, logging, alert email and FortiGuard updates.
- C. Each VDM can run different firmware versions.
- D. Administrative users with a 'super\_admin' profile can administrate only one VDM.

**Correct Answer: AB**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 122**

Which of the following statements is correct concerning multiple vdoms configured in a FortiGate device?

- A. FortiGate devices, from the FGT/FWF 60D and above, all support VDMs.
- B. All FortiGate devices scale to 250 VDMs.
- C. Each VDM requires its own FortiGuard license.
- D. FortiGate devices support more NAT/route VDMs than Transparent Mode VDMs.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 123**

A FortiGate unit has multiple VDMs in NAT/route mode with multiple VLAN interfaces in each VDM. Which of the following statements is correct regarding the IP addresses assigned to each VLAN interface?

- A. Different VLANs can share the same IP address as long as they have different VLAN IDs.

- B. Different VLANs can share the same IP address as long as they are in different physical interface.
- C. Different VLANs can share the same IP address as long as they are in different VDOMs.
- D. Different VLANs can never share the same IP addresses.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 124

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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 125

A FortiGate devices is configured with four VDOMs: 'root' and 'vdom1' are in NAT/route mode; 'vdom2' and 'vdom2' are in transparent mode. The management VDOM is 'root'. Which of the following statements are true? (Choose two.)

- A. An inter-VDOM link between 'root' and 'vdom1' can be created.
- B. An inter-VDOM link between 'vdom1' and vdom2' can created.
- C. An inter-VDOM link between 'vdom2' and vdom3' can created.
- D. Inter-VDOM link links must be manually configured for FortiGuard traffic.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 126**

Which of the following statements is true regarding a FortiGate device operating in transparent mode? ( Choose three.)

- A. It acts as a layer 2 bridge
- B. It acts as a layer 3 router
- C. It forwards frames using the destination MAC address.
- D. It forwards packets using the destination IP address.
- E. It can perform content inspection (antivirus, web filtering, etc)

**Correct Answer:** ACE

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 127**

Which of the following statements are correct concerning IPsec dialup VPN configurations for FortiGate devices? (Choose two)

- A. Main mode must be used when there is no more than one IPsec dialup VPN configured on the same FortiGate device.
- B. A FortiGate device with an IPsec VPN configured as dialup can initiate the tunnel connection to any remote IP address.
- C. Peer ID must be used when there is more than one aggressive-mode IPsec dialup VPN on the same FortiGate device.
- D. The FortiGate will automatically add a static route to the source quick mode selector address received from each remote peer.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 128**

Which of the following combinations of two FortiGate device configurations (side A and side B), can be used to successfully establish an IPsec VPN between them? (choose two)

- A. Side A: main mode, remote gateway as static IP address, policy based VPN. Side B: aggressive mode, remote Gateway as static IP address policy-based VPN.

- B. Side A: main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as static IP address, route-based VPN
- C. Side A: main mode, remote gateway as static IP address, policy based VPN. Side B: main mode, remote gateway as dialup, route-based VPN.
- D. Side A: main mode, remote gateway as dialup policy based VPN, Side B: main mode, remote gateway as dialup, policy based VPN.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 129

Which of the following statements are correct differences between NAT/route and transparent mode? (Choose two.)

- A. In transparent mode, interfaces do not have IP addresses.
- B. Firewall policies are only used in NAT/ route mode.
- C. Static routers are only used in NAT/route mode.
- D. Only transparent mode permits inline traffic inspection at layer 2.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 130

Which of the following are operating mode supported in FortiGate devices? (Choose two)

- A. Proxy
- B. Transparent
- C. NAT/route
- D. Offline inspection

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 131**

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 FortiGate interfaces port1 and port2.
- D. The FortiGate devices configured in transparent mode.

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 132**

Which of the following statement correct describes the use of the "diagnose sys ha reset-uptime" command?

- A. To force an HA failover when the HA override setting is disabled.
- B. To force an HA failover when the HA override setting is enabled.

- C. To clear the HA counters.
- D. To restart a FortiGate unit that is part of an HA cluster.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 133**

What are required to be the same for two FortiGate units to form an HA cluster? (Choose two)

- A. Firmware.
- B. Model.
- C. Hostname.
- D. System time zone.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 134**

Which of the following statements describes the objectives of the gratuitous ARP packets sent by an HA cluster?

- A. To synchronize the ARP tables in all the FortiGate Units that are part of the HA cluster.
- B. To notify the network switches that a new HA master unit has been elected.
- C. To notify the master unit that the slave devices are still up and alive.
- D. To notify the master unit about the physical MAC addresses of the slave units.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 135**

Which of the following statements are correct regarding a master HA unit? (Choose two)

- A. There should be only one master unit in each HA virtual cluster.
- B. The Master synchronizes cluster configuration with slaves.
- C. Only the master has a reserved management HA interface.
- D. Heartbeat interfaces are not required on a master unit.

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 136**

Which statement describes how traffic flows in sessions handled by a slave unit in an active-active HA cluster?

- A. Packets are sent directly to the slave unit using the slave physical MAC address.
- B. Packets are sent directly to the slave unit using the HA virtual MAC address.
- C. Packets arrived at both units simultaneously, but only the slave unit forwards the session.
- D. Packets are first sent to the master unit, which then forwards the packets to the slave unit.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 137**

Which of the following statements are correct concerning the FortiGate session life support protocol? (Choose two)

- A. By default, UDP sessions are not synchronized.
- B. Up to four FortiGate devices in standalone mode are supported.
- C. Only the master unit handles the traffic.
- D. Allows per-VDOM session synchronization.

**Correct Answer:** AD

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 138**

What is the default criteria for selecting the HA master unit in a HA cluster?

- A. port monitor, priority, uptime, serial number
- B. Port monitor, uptime, priority, serial number
- C. Priority, uptime, port monitor, serial number
- D. uptime, priority, port monitor, serial number

**Correct Answer:** B

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 139**

What information is synchronized between two FortiGate units that belong to the same HA cluster? (Choose three)

- A. IP addresses assigned to DHCP enabled interface.
- B. The master devices hostname.
- C. Routing configured and state.
- D. Reserved HA management interface IP configuration.
- E. Firewall policies and objects.

**Correct Answer:** ACE

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 140**

Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)

### Peer Options

Accept Types

This peer ID ▼

Peer ID

fortinet

### Phase 1 Proposal

+ Add

Encryption

3DES ▼

Authentication

SHA1 ▼

Diffie-Hellman Groups

☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16

☐ 15 ☒ 14 ☒ 5 ☐ 2 ☐ 1

Key Lifetime (seconds)

86400

Local ID

### XAUTH

Type

Disabled ▼

### Phase 2 Selectors

Name

Local Address

Remote Address

+ Add

0.0.0.0/0.0.0.0

0.0.0.0/0.0.0.0



- A. The quick mode selector in the remote site must also be 0.0.0.0/0 for the source and destination addresses.
- B. Only remote peers with the peer ID 'fortinet' will be able to establish a VPN.
- C. The FortiGate device will automatically add a static route to the source quick mode selector address received from each remote VPN peer.
- D. The configuration will work only to establish FortiClient-to-FortiGate tunnels. A FortiGate tunnel requires a different configuration.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 141

The exhibit shows a part output of the diagnostic command 'diagnose debug application ike 255', taken during establishment of a VPN. Which of the following statement are correct concerning this output? (choose two)

```
Ike 0:Remote:7:22: responder received first quick-mode message
ike 0:Remote:7:22: peer proposal is: peer:0:0.0.0.0-255.255.255.255:0, me:0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7: sent IKE msg (quick_r1send): 172.20.186.222:500->172.20.187.114:500, len=356
ike 0: comes 172.20.187.114:500->172.20.186.222:500, ifindex=2....
ike 0:Remote:7:P2:22: replay protection enabled
ike 0:Remote:7:P2:22: SA life soft seconds=1750.
ike 0:Remote:7:P2:22: SA life hard seconds=1800.
ike 0:Remote:7:P2:22: IPsec SA selectors #src=1 #dst=1
ike 0:Remote:7:P2:22: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: dst 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:Remote:7:P2:22: add IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: added IPsec SA: SPIs=6e13ca19/8f1ce9ae
ike 0:Remote:7:P2:22: sending SNMP tunnel UP trap
```

- A. The quick mode selectors negotiated between both IPsec VPN peers is 0.0.0.0/32 for both source and destination addresses.
- B. The output corresponds to a phase 2 negotiation
- C. NAT-T enabled and there is third device in the path performing NAT of the traffic between both IPsec VPN peers.
- D. The IP address of the remote IPsec VPN peer is 172.20.187.114

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 142**

What is required in a FortiGate configuration to have more than one dialup IPsec VPN using aggressive mode?

- A. All the aggressive mode dialup VPNs MUST accept connections from the same peer ID.
- B. Each peer ID MUST match the FQDN of each remote peer.
- C. Each aggressive mode dialup MUST accept connections from different peer ID.
- D. The peer ID setting must NOT be used.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 143**

Which of the following statements are correct concerning IKE mode config? (Choose two)

- A. It can dynamically assign IP addresses to IPsec VPN clients.
- B. It can dynamically assign DNS settings to IPsec VPN clients.
- C. It uses the ESP protocol.
- D. It can be enabled in the phase 2 configuration.

**Correct Answer: AB**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 144**

Which statement is correct concerning an IPsec VPN with the remote gateway setting configured as 'Dynamic DNS'?

- A. The FortiGate will accept IPsec VPN connection from any IP address.
- B. The FQDN resolution of the local FortiGate IP address where the VPN is terminated must be provided by a dynamic DNS provider.
- C. The FortiGate will Accept IPsec VPN connections only from IP addresses included on a dynamic DNS access list.
- D. The remote gateway IP address can change dynamically.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 145**

Which of the following protocols are defined in the IPsec Standard? (Choose two)

- A. AH
- B. GRE
- C. SSL/TLS
- D. ESP

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



**QUESTION 146**

What configuration objects are automatically added when using the FortiGate's FortiClient VPN Configurations Wizard?(Choose two)

- A. Static route
- B. Phase 1
- C. Users group
- D. Phase 2

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 147**

Which of the following statements are correct concerning layer 2 broadcast domains in transparent mode VDOMs?(Choose two)

- A. The whole VDOM is a single broadcast domain even when multiple VLAN are used.

- B. Each VLAN is a separate broadcast domain.
- C. Interfaces configured with the same VLAN ID can belong to different broadcast domains.
- D. All the interfaces in the same broadcast domain must use the same VLAN ID.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.firewallshop.com/download/fortinet/FortiGate\\_VLANs\\_and\\_VDOMs\\_Guide.pdf](http://www.firewallshop.com/download/fortinet/FortiGate_VLANs_and_VDOMs_Guide.pdf)

#### QUESTION 148

Which of the following statements is correct regarding FortiGate interfaces and spanning tree protocol? (Choose Two)

- A. Only FortiGate switch interfaces Participate in spanning tree.
- B. All FortiGate interfaces in transparent mode VDOMs participate in spanning tree.
- C. All FortiGate interfaces in NAT/route mode VDOMs Participate in spanning tree.
- D. All FortiGate interfaces in transparent mode VDOMs may block or forward BPDUs.

**Correct Answer:** BD

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### QUESTION 149

On your FortiGate 60D, you've configured firewall policies. They port forward traffic to your Linux Apache web server. Select the best way to protect your web server by using the IPS engine.

- A. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache applications. Configured DLP to block HTTP GET request with credit card numbers.
- B. Enable IPS signatures for Linux servers with HTTP, TCP and SSL protocols and Apache applications. Configure DLP to block HTTP GET with credit card numbers. Also configure a DoS policy to prevent TCP SYN floods and port scans.
- C. None. FortiGate 60D is a desktop model, which does not support IPS.
- D. Enable IPS signatures for Linux and windows servers with FTP, HTTP, TCP, and SSL protocols and Apache and PHP applications.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/2181/fortigate-security-profiles-guide-524.pdf>

**QUESTION 150**

Which changes to IPS will reduce resource usage and improve performance? (Choose three)

- A. In custom signature, remove unnecessary keywords to reduce how far into the signature tree that FortiGate must compare in order to determine whether the packet matches.
- B. In IPS sensors, disable signatures and rate based statistics (anomaly detection) for protocols, applications and traffic directions that are not relevant.
- C. In IPS filters, switch from 'Advanced' to 'Basic' to apply only the most essential signatures.
- D. In firewall policies where IPS is not needed, disable IPS.
- E. In firewall policies where IPS is used, enable session start logs.

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 151**

Which statement concerning IPS is false?

- A. IPS packages contain an engine and signatures used by both IPS and other flow-based scans.
- B. One-arm topology with sniffer mode improves performance of IPS blocking.
- C. IPS can detect zero-day attacks.
- D. The status of the last service update attempt from FortiGuard IPS is shown on System>Config>FortiGuard and in output from 'diag autoupdate version'

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 152**

Which best describes the mechanism of a TCP SYN flood?

- A. The attackers keeps open many connections with slow data transmission so that other clients cannot start new connections.



- B. The attackers sends a packets designed to sync with the FortiGate
- C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
- D. The attacker starts many connections, but never acknowledges to fully form them.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 153**

Which profile could IPS engine use on an interface that is in sniffer mode? (Choose three)

- A. Antivirus (flow based)
- B. Web filtering (PROXY BASED)
- C. Intrusion Protection
- D. Application Control
- E. Endpoint control

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://www.fortinet.com/sites/default/files/productdatasheets/fortios-5-4-datasheet\\_2.pdf](https://www.fortinet.com/sites/default/files/productdatasheets/fortios-5-4-datasheet_2.pdf) (page 10 - offline inspection)

#### **QUESTION 154**

Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (choose three)

- A. Irix
- B. QNIX
- C. Linux
- D. Mac OS
- E. BSD

**Correct Answer:** CDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://docs.fortinet.com/uploaded/files/1082/fortigate-security\\_profiles-50.pdf](http://docs.fortinet.com/uploaded/files/1082/fortigate-security_profiles-50.pdf) (page 59)

**QUESTION 155**

You are creating a custom signature. Which has incorrect syntax?

- A. F-SBID(--attack\_id 1842,--name "Ping.Death";--protocol icmp; --data\_size>32000;)
- B. F-SBID(--name "Block.SMTP.VRFY.CMD";--pattern "vrfy";-- service SMTP; --no\_case;--context header;)
- C. F-SBID(--name "Ping.Death";--protocol icmp;--data\_size>32000;)
- D. F-SBID(--name "Block".HTTP.POST"; --protocol tcp;-- service HTTP;-- flow from\_client; --pattern "POST"; -- context uri;--within 5,context;)

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://forum.fortinet.com/tm.aspx?m=110493>

**QUESTION 156**

Which best describe the mechanism of a TCP SYN flood?

- A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.
- B. The attacker sends a packet designed to "sync" with the FortiGate.
- C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
- D. The attacker starts many connections, but never acknowledges to fully form them.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 157**

Which statement is correct concerning creating a custom signature?

- A. It must start with the name
- B. It must indicate whether the traffic flow is from the client or the server.
- C. It must specify the protocol. Otherwise, it could accidentally match lower-layer protocols.
- D. It is not supported by Fortinet Technical Support.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 158**

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.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 159**

What are the advantages of FSSO DC mode over polling mode?

- A. Redundancy in the collector agent.
- B. Allows transparent authentication.
- C. DC agents are not required in the AD domain controllers.
- D. Scalability

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 160**

Which of the following statements are correct about NTLM authentication? (Choose three)

- A. NTLM negotiation starts between the FortiGate device and the user's browser.
- B. It must be supported by the user's browser.
- C. It must be supported by the domain controllers.
- D. It does not require a collector agent.
- E. It does not require DC agents.

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 161**

Which of the following statements best describes how the collector agent learns that a user has logged off from the network?

- A. The workstation fails to reply to the polls frequently done by the collector agent.
- B. The DC agent captures the log off event from the event logs, which it forwards to the collector agent.
- C. The work station notifies the DC agent that the user has logged off.
- D. The collector agent gets the logoff events when polling the respective domain controller.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 162**

Which of the following statements best describes the role of a DC agents in an FSSO DC?

- A. Captures the login events and forward them to the collector agent.
- B. Captures the user IP address and workstation name and forward that information to the FortiGate devices.
- C. Captures the login and logoff events and forward them to the collector agent.
- D. Captures the login events and forward them to the FortiGate devices.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 163**

Which of the following FSSO modes must be used for Novell eDirectory networks?

- A. Agentless polling
- B. LDAP agent
- C. eDirectory agent
- D. DC agent

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/1041/fortigate-authentication-40-mr3.pdf> (page 140)

**QUESTION 164**

In a FSSO agentless polling mode solution, where must the collector agent be?

- A. In any Windows server
- B. In any of the AD domain controllers
- C. In the master AD domain controller
- D. The FortiGate device polls the AD domain controllers

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 165**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: e <http://kb.fortinet.com/kb/documentLink.do?externalID=FD30964>

#### **QUESTION 166**

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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 167**

In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

- A. The DC agents get each user IP address from the event logs and forward that information to the collector agent
- B. The collector agent does not know, and does not need, each user IP address. Only workstation names are known by the collector agent.
- C. The collector agent frequently polls the AD domain controllers to get each user IP address.
- D. The DC agent learns the workstation name from the event logs and DNS is then used to translate those names to the respective IP addresses.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 168**

Which FSSO agents are required for a FSSO agent-based polling mode solution?

- A. Collector agent and DC agents
- B. Polling agent only
- C. Collector agent only
- D. DC agents only

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 169**

Which of the following statements are true about Man-in-the-middle SSL Content Inspection? (Choose three.)

- A. The FortiGate device “re-signs” all the certificates coming from the HTTPS servers
- B. The FortiGate device acts as a sub-CA
- C. The local service certificate of the web server must be installed in the FortiGate device
- D. The FortiGate device does man-in-the-middle inspection.
- E. The required SSL Proxy certificate must first be requested to a public certificate authority (CA).

**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 170**

Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

- A. In symmetric cryptography, the keys are publicly available. In asymmetric cryptography, the keys must be kept secret.
- B. Asymmetric cryptography can encrypt data faster than symmetric cryptography
- C. Symmetric cryptography uses one pre-shared key. Asymmetric cryptography uses a pair of keys
- D. Asymmetric keys can be sent to the remote peer via digital certificates. Symmetric keys cannot

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 171**

Which of the following statements best describes what a Public Certificate Authority (CA) is?

- A. A service that provides a digital certificate each time a user is authenticating
- B. An entity that certifies that the information contained in a digital certificate is valid and true.
- C. The FortiGate process in charge of generating digital certificates on the fly for SSL inspection purposes
- D. A service that validates digital certificates for certificate-based authentication purposes

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 172**

Which of the following statements are true about the SSL Proxy certificate that must be used for SSL Content Inspection? (Choose two.)

- A. It cannot be signed by a private CA
- B. It must have either the field "CA=True" or the field "Key Usage=KeyCertSign"
- C. It must be installed in the FortiGate device
- D. The subject field must contain either the FQDN, or the IP address of the FortiGate device

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 173**

Which of the following statements are true about PKI users created in a FortiGate device? (Choose two.)

- A. Can be used for token-based authentication
- B. Can be used for two-factor authentication
- C. Are used for certificate-based authentication



D. Cannot be members of user groups

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/1937/fortigate-authentication-52.pdf> (page 14)

#### **QUESTION 174**

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)

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 175**

Which of the following actions can be used to back up the keys and digital certificates in a FortiGate device? (Choose two.)

- A. Taking a full backup of the FortiGate configuration
- B. Uploading a PKCS#10 file to a USB drive
- C. Manually uploading the certificate information to a Certificate authority (CA)
- D. Uploading a PKCS#12 file to a TFTP server

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 176**

Which of the following statements must be true for a digital certificate to be valid? (Choose two.)

- A. It must be signed by a “trusted” CA
- B. It must be listed as valid in a Certificate Revocation List (CRL)
- C. The CA field must be “TRUE”
- D. It must be still within its validity period

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 177**

Of the following information, what can be recorded by a Data Leak Prevention sensor configured to do a summary archiving? (Choose three.)

- A. Visited URL (for the case of HTTP traffic)
- B. Sender email address (for the case of SMTP traffic)
- C. Recipient email address (for the case of SMTP traffic)
- D. Attached file (for the case of SMTP traffic)
- E. Email body (for the case of SMTP traffic)



**Correct Answer:** BCE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/1084/fortigate-loggingreporting-509.pdf>

#### **QUESTION 178**

Which of the following statements best describes what the Document Fingerprinting feature is for?

- A. Protects sensitive documents from leakage
- B. Appends a fingerprint signature to all documents sent by users
- C. Appends a fingerprint signature to all the emails sent by users
- D. Validates the fingerprint signature in users' emails

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/2181/fortigate-security-profiles-guide-524.pdf> (133)

**QUESTION 179**

Which action is taken by the FortiGate device when a file matches more than one rule in a Data Leak Prevention sensor?

- A. The actions specified by the rule that most specifically matched the file
- B. The actions specified in the first rule from top to bottom
- C. All actions specified by all the matched rules.
- D. The actions specified in the rule with the higher priority number

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 180**

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

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://kb.fortinet.com/kb/documentLink.do?externalID=FD35108>

**QUESTION 181**

Which of the following actions that can be taken by the Data Leak Prevention scanning? (Choose three.)

- A. Block
- B. Reject
- C. Tag

- D. Log only
- E. Quarantine IP address

**Correct Answer:** ADE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/2181/fortigate-security-profiles-guide-524.pdf> (131)

#### **QUESTION 182**

Which of the following network protocols can be inspected by the Data Leak Prevention scanning? (Choose three.)

- A. SMTP
- B. HTTP-POST
- C. AIM
- D. MAPI
- E. ICQ

**Correct Answer:** ABD

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### **QUESTION 183**

What types of troubleshooting can you do when uploading firmware? (Choose two.)

- A. Investigate corrupted firmware
- B. Investigate current runtime state
- C. Investigate damaged hardware
- D. Investigate configuration history

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 184**

Which are outputs for the command 'diagnose hardware deviceinfo nic'? (Choose two.)

- A. ARP cache
- B. Physical MAC address
- C. Errors and collisions
- D. Listening TCP ports

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/1067/fortigate-troubleshooting-40-mr2.pdf> (page 28)

**QUESTION 185**

In FortiOS session table output, what is the correct 'proto\_state' number for an established, non-proxied TCP connection?

- A. 00
- B. 11
- C. 01
- D. 05



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 186**

Which commands are appropriate for investigating high CPU? (Choose two.)

- A. diag sys top
- B. diag hardware sysinfo mem
- C. diag debug flow
- D. get system performance status

**Correct Answer:** AD

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/1067/fortigate-troubleshooting-40-mr2.pdf> (109)

**QUESTION 187**

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**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <http://docs.fortinet.com/uploaded/files/1067/fortigate-troubleshooting-40-mr2.pdf> (33. 34)

**QUESTION 188**

Which TCP states does the global setting 'tcp-half-open-timer' applies to? (Choose two.)

- A. SYN SENT
- B. SYN & SYN/ACK
- C. FIN WAIT
- D. TIME WAIT

**Correct Answer: AD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 189**

In FortiOS session table output, what are the two possible 'proto\_state' values for a UDP session? (Choose two.)

- A. 00

- B. 11
- C. 01
- D. 05

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 190**

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.

**Correct Answer:** A

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### **QUESTION 191**

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

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 192**

Which of the following statements best describe the main requirements for a traffic session to be offload eligible to an NP6 processor? (Choose three.)

- A. Session packets do NOT have an 802.1Q VLAN tag.
- B. It is NOT multicast traffic.
- C. It does NOT require proxy-based inspection.
- D. Layer 4 protocol must be UDP, TCP, SCTP or ICMP.
- E. It does NOT require flow-based inspection.

**Correct Answer:** CDE

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 193**

Which statement best describes what a Fortinet System on a Chip (SoC) is?

- A. Low-power chip that provides general purpose processing power
- B. Chip that combines general purpose processing power with Fortinet's custom ASIC technology
- C. Light-version chip (with fewer features) of an SP processor
- D. Light-version chip (with fewer features) of a CP processor

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.fortinet.com/press\\_releases/100713.html](http://www.fortinet.com/press_releases/100713.html)

**QUESTION 194**

Which of the following statements are true regarding traffic accelerated by an NP processor? (Choose two.)

- A. TCP SYN packets are always handled by the NP Processor
- B. The initial packets go to the NP Processor, where a decision is taken on if the session can be offloaded or not.
- C. Packets for a session termination are always handled by the CPU.
- D. The initial packets go to the CPU, where a decision is taken on if the session can be offloaded or not.



**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

