

NSE5 fortinet

Number: NSE5
Passing Score: 800
Time Limit: 120 min



NSE 5 - FortiGate Network Security Management and Analysis



Exam A**QUESTION 1**

In which order are firewall policies processed on a FortiGate unit?

- A. From top to bottom, according with their sequence number.
- B. From top to bottom, according with their policy ID number.
- C. Based on best match.
- D. Based on the priority value.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

What logging options are supported on a FortiGate unit? (Choose two.)

- A. LDAP
- B. Syslog
- C. FortiAnalyzer
- D. SNMP



Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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 4

With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.

If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

- A. The login event is sent to a collector agent by the DC agent.
- B. the login event is sent to the FortiGate by the DC agent.
- C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.
- D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 5

Regarding the use of web-only mode SSL VPN, which statement is correct?

- A. It support SSL version 3 only.
- B. It requires a Fortinet-supplied plug-in on the web client.
- C. It requires the user to have a web browser that supports 64-bit cipher length.
- D. The JAVA run-time environment must be installed on the client.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: http://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR1/Fortigate-SSLVPN's_FortiOS_Handbook_4.0_MR1.pdf
page 18

QUESTION 6

Review the IPsec diagnostics output of the command `diagnose vpn tunnel list` shown in the exhibit below.

```
STUDENT # diagnose vpn tunnel list
list all ipsec tunnel in vd 0
-----
name=FClient_0 ver=1 serial=3 10.200.1.1:4500->10.200.3.1:64916 lgwy=static tun=intf mode=dial_
parent=FClient index=0
proxyid_num=1 child_num=0 refcnt=8 ilast=2 olast=2
stat: rxp=59 txp=0 rxb=15192 txb=0
dpd: mode=active on=1 idle=5000ms retry=3 count=0 seqno=10
natt: mode=keepalive draft=32 interval=10 remote_port=64916
proxyid=FClient proto=0 sa=1 ref=2 auto_negotiate=0 serial=1
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:172.20.1.1-172.20.1.1:0
  SA: ref=3 options=00000006 type=00 soft=0 mtu=1280 expire=1717 replaywin=1024 seqno=1
  life: type=01 bytes=0/0 timeout=1791/1800
  dec: spi=a29046e9 esp=3des key=24 0525830c6fd67ca37e9d6dad174d175e24f97c3b87f428fa
      ah=sha1 key=20 982f8ba194f3f797773efc605c8321b728dabf1d
  enc: spi=19be4052 esp=3des key=24 da597cb7fec913528f8598d1aa7ecd17156a2a7a4afeeb4c
      ah=sha1 key=20 9e2c5d0fc055fa0149bc66024732e9a85bbe8016
-----
```

Which statements are correct regarding this output (Choose two.)

- A. The connecting client has been allocated address 172.20.1.1.
- B. In the Phase 1 settings, dead peer detection is enabled.
- C. The tunnel is idle.
- D. The connecting client has been allocated address 10.200.3.1.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

If there are no changes in the routing table and in the case of TCP traffic, which of the following correctly describes the routing table lookups performed by a FortiGate in NAT /Route mode, when searching for a suitable gateway?

- A. A lookup is done only when the first packet coming from the client (SYN) arrives.
- B. A lookup is done when the first packet coming from the client (SYN) arrives, and a second one is performed when the first packet coming from the server (SYN/ACK) arrives.
- C. Three lookups are done during the TCP 3-way handshake (SYN, SYN/ACK, ACK).
- D. A lookup is always done each time a packet arrives, from either the server or the client side.

Correct Answer: B

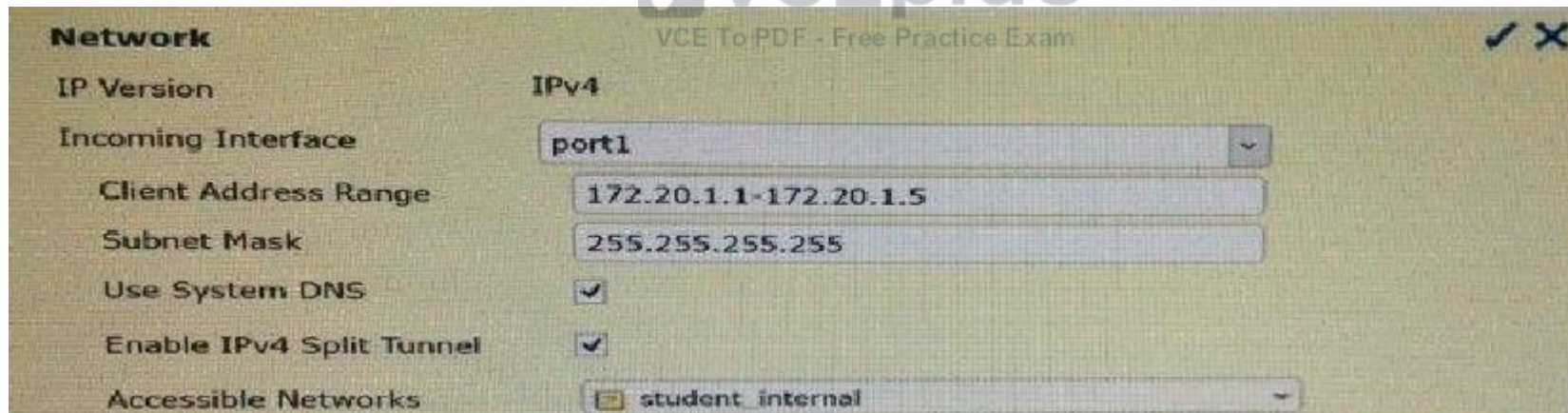
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Review the configuration for FortiClient IPsec shown in the exhibit.



Network

IP Version: IPv4

Incoming Interface: port1

Client Address Range: 172.20.1.1-172.20.1.5

Subnet Mask: 255.255.255.255

Use System DNS: ☒

Enable IPv4 Split Tunnel: ☒

Accessible Networks: student_internal

Which statement is correct regarding this configuration?

- A. The connecting VPN client will install a route to a destination corresponding to the student internal address object.
- B. The connecting VPN client will install a default route.
- C. The connecting VPN client will install a route to the 172.20.1.[1-5] address range.

D. The connecting VPN client will connect in web portal mode and no route will be installed.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

You are the administrator in charge of a point-to-point IPsec VPN between two FortiGate units using route based mode. Users from either side must be able to initiate new sessions with no restrictions. There is only 1 subnet at either end and the FortiGate already has a default route.

Which two configuration steps are required in each FortiGate to achieve these objectives? (Choose two.)

- A. Create one firewall policy.
- B. Create two firewall policies.
- C. Add a route to the remote subnet.
- D. Add two IPsec phases 2.

Correct Answer: BC

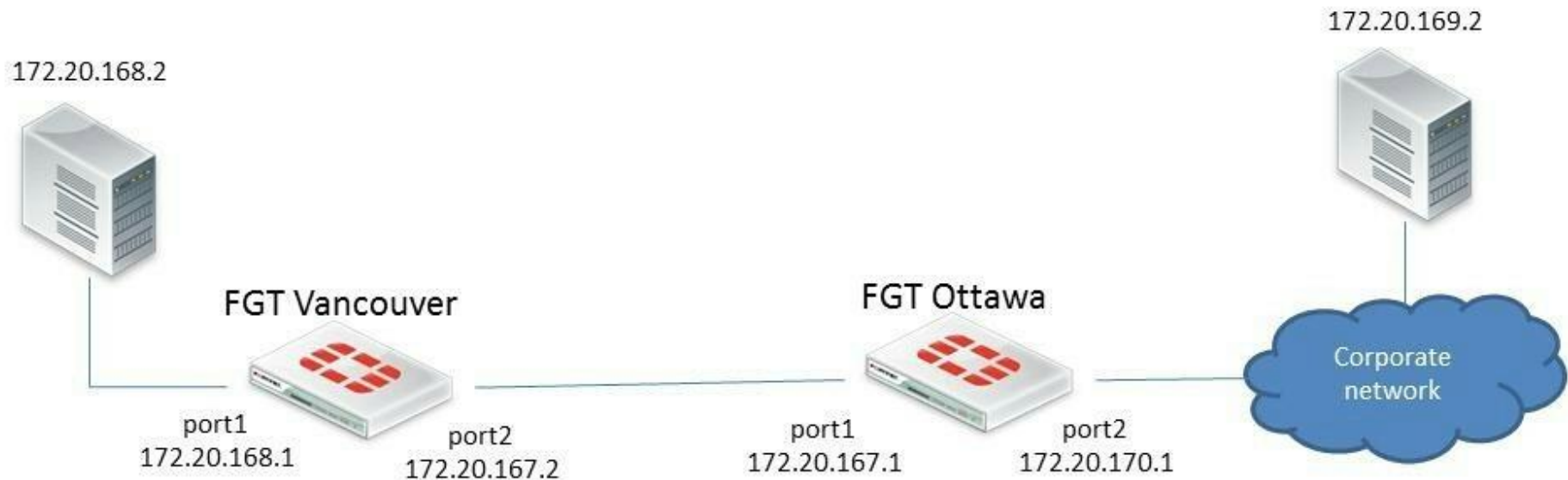
Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

Examine the exhibit below; then answer the question following it.



In this scenario. The FortiGate unit in Ottawa has the following routing table:

```
s* 0.0.0.0/0 [10/0] via 172.20.170.254, port2
c 172.20.167.0/24 is directly connected, port1
c 172.20.170.0/24 is directly connected, port2
```

Sniffer tests show that packets sent from the source IP address 172.20.168.2 to the destination IP address 172.20.169.2 are being dropped by the FortiGate located in Ottawa. Which of the following correctly describes the cause for the dropped packets?

- A. The forward policy check.
- B. The reserve path forwarding check.
- C. The subnet 172.20.169.0/24 is NOT in the Ottawa FortiGate's routing table.
- D. The destination workstation 172.20.169.2 does NOT have the subnet 172.20.168.0/24 in its routing table.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

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 12

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 13

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 14

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 15

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

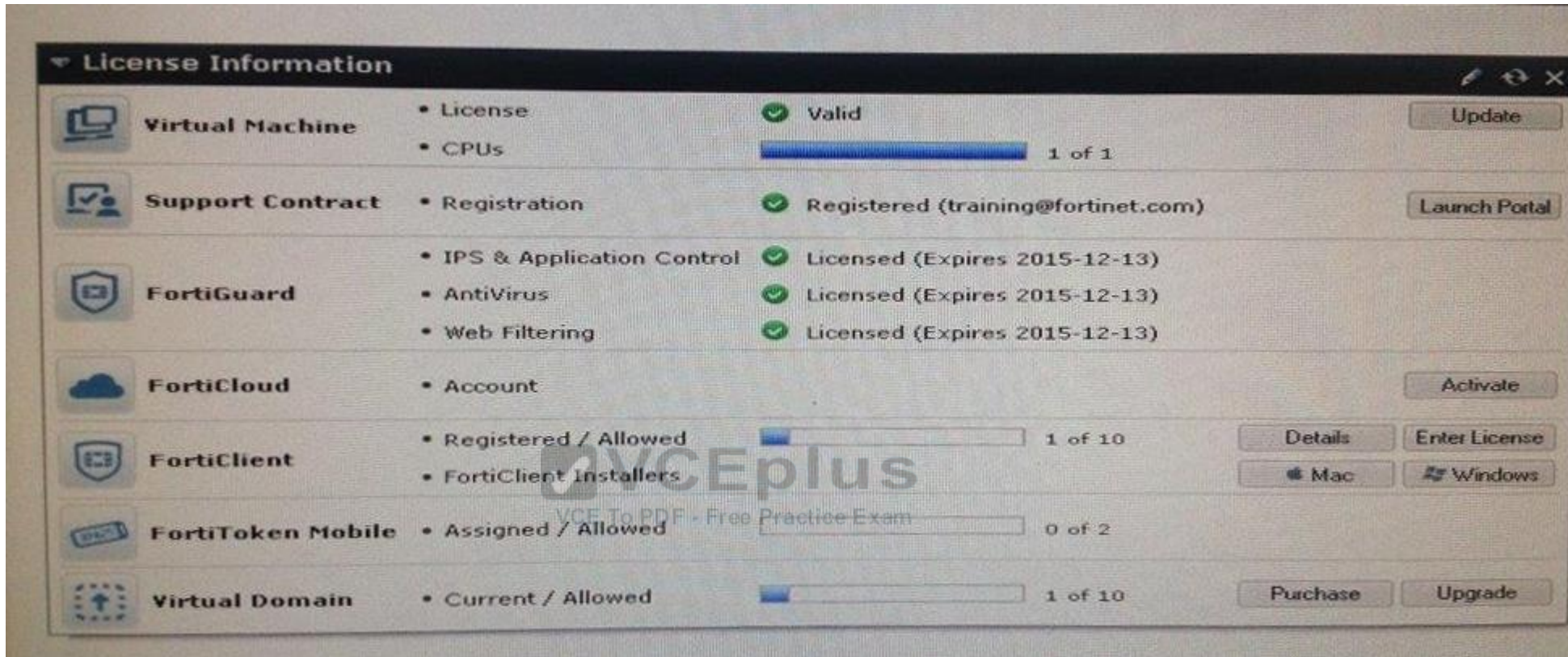
Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

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 17**

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 18**

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

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 19

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 20

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 21

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 22

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 23

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 24

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 25

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 26**

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 27**

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 28**

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 29

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 30

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 31

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 32

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: AD

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 33

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 34

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 35**

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 36**

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 37**

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 38

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 39

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 40

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 41

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 42

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 43

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 44

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 45

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 46

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 47

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 48

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 49

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 50

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 51

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 52

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 53

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 54

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 55

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 56

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 57

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 58**

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 59**

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 60**

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 61

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 62

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 63

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 64

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 65

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 66

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 67

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 68

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 69

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: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

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 71**

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 72**

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 73**

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 74

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 75

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 76

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 77

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 78

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 79

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 80

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 81

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 82

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 83

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 84

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 85

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 86

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 87

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

```
# 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 88

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 89

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 90

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 91

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 92

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 93

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 94

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 95

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 96

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 97

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 VDMs.
- D. Different VLANs can never share the same IP addresses.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 98

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 compliant switches.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 99

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 100

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 101

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 102

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 103

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 104

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 105

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 106

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 107

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 108

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 109

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

QUESTION 110

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 111

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 112

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 113

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 114

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 115

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 (page 10 - offline inspection)

QUESTION 116

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 (page 59)

QUESTION 117

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 118

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 119

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 120

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 121

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 122

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 123

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 124

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 125

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: