QUESTION 15
Which two statements are correct about NGFW Policy-based mode? (Choose two.)

A. NGFW policy-based mode does not require the use of central source NAT policy
B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
D. NGFW policy-based mode policies support only flow inspection

Correct Answer: CD

QUESTION 16
Which three statements about a flow-based antivirus profile are correct? (Choose three.)

A. IPS engine handles the process as a standalone.
B. FortiGate buffers the whole file but transmits to the client simultaneously.
C. If the virus is detected, the last packet is delivered to the client.
D. Optimized performance compared to proxy-based inspection.
E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

Correct Answer: BDE

QUESTION 17
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time
B. FortiGuaid update servers
C. Operating mode
D. NGFW mode

Correct Answer: CD

QUESTION 18
Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Correct Answer: BC

QUESTION 19
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache
B. FortiSIEM

C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Correct Answer: BCE

QUESTION 20
FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax. Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

A. www.example.com:443
B. www.example.com
C. example.com
D. www.example.com/index.html

Correct Answer: BC

QUESTION 21
An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

A. Policy lookup will be disabled.
B. By Sequence view will be disabled.
C. Search option will be disabled
D. Interface Pair view will be disabled.

Correct Answer: D

QUESTION 22
An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value. Which timeout option should be configured on FortiGate?

A. auth-on-demand
B. soft-timeout
C. idle-timeout
D. new-session
E. hard-timeout

Correct Answer: E

QUESTION 23
Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

A. FortiGate uses the AD server as the collector agent.
B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
C. FortiGate does not support workstation check.
D. FortiGate directs the collector agent to use a remote LDAP server.

Correct Answer: BD

QUESTION 24
A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service. What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

A. Static IP Address
B. Dialup User
C. Dynamic DNS
D. Pre-shared Key

Correct Answer: B

QUESTION 25
Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache
B. FortiGate hostname
C. NTP
D. DNS

Correct Answer: CD

QUESTION 26
Which two statements are true about the FGCP protocol? (Choose two.)

A. Not used when FortiGate is in Transparent mode
B. Elects the primary FortiGate device
C. Runs only over the heartbeat links
D. Is used to discover FortiGate devices in different HA groups

Correct Answer: BC

QUESTION 27
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status
B. get system performance status
C. diagnose sys top
D. get system arp

Correct Answer: D

QUESTION 28
An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

A. The strict RPF check is run on the first sent and reply packet of any new session.
B. Strict RPF checks the best route back to the source using the incoming interface.
C. Strict RPF checks only for the existence of at cast one active route back to the source using the

incoming interface.
D. Strict RPF allows packets back to sources with all active routes.

Correct Answer: B

QUESTION 29
Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.
B. It is available only on a proxy-based firewall policy.
C. It inspects video files hosted on file sharing services.
D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Correct Answer: B

QUESTION 30
Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)

A. Proxy-based inspection
B. Certificate inspection
C. Flow-based inspection
D. Full Content inspection

Correct Answer: AC

QUESTION 31
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

- All traffic must be routed through the primary tunnel when both tunnels are up
- The secondary tunnel must be used only if the primary tunnel goes down
- In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
B. Enable Dead Peer Detection .
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Correct Answer: BC

QUESTION 32
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

A. Add the support of NTLM authentication.
B. Add user accounts to Active Directory (AD).