Fortinet.Premium.NSE4_FGT-7.2.30q - DEMO

Number: NSE4_FGT-7.2
Passing Score: 800
Time Limit: 120 min

Exam Code: NSE4_FGT-7.2
Exam Name: Fortinet NSE 4 - FortiOS 7.2
Website: https://VCEup.com/
Team-Support: Support@VCEup.com

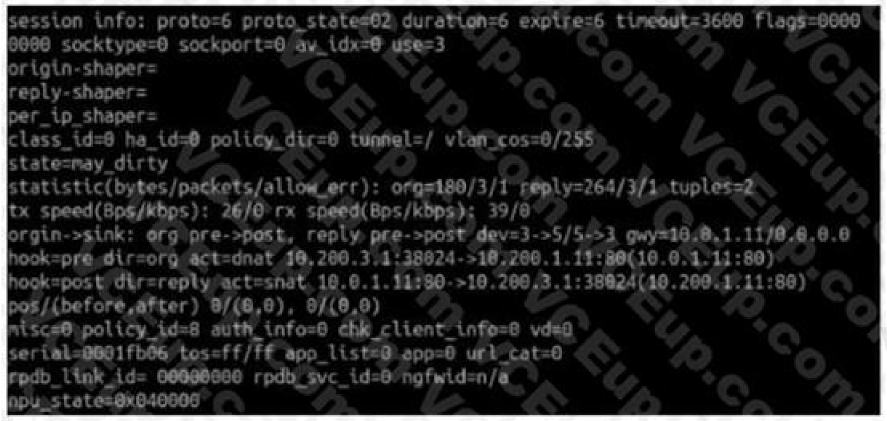
QUESTION 1
Which two statements are correct about NGFW Policy-based mode? (Choose two.)

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
Refer to the exhibit.



```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

A. The session is in SYN_SENT state.
B. The session is in FIN_ACK state.
C. The session is in FTN_WAIT state.
D. The session is in ESTABLISHED state.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Indicates TCP (proto=6) session in SYN_SENT state (proto=state=2)
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

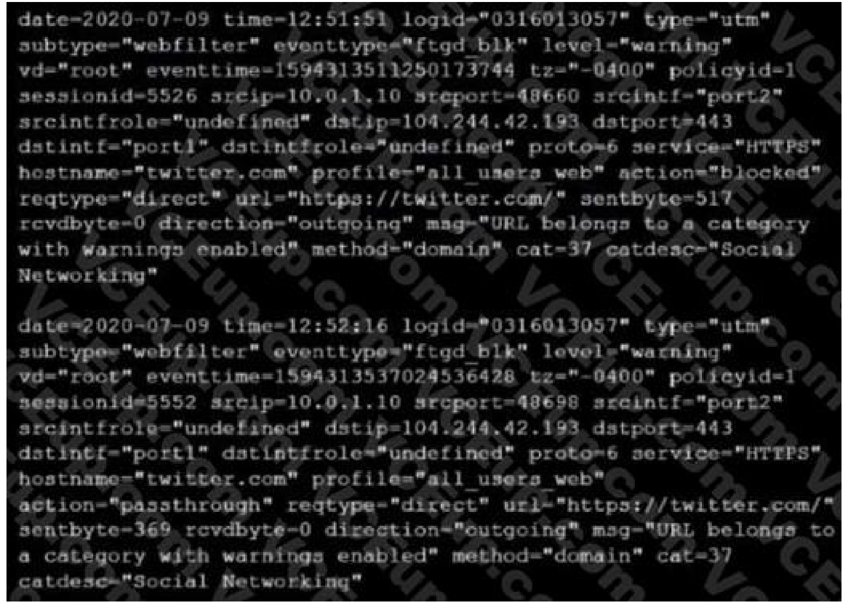
QUESTION 3
Which two statements explain antivirus scanning modes? (Choose two.)

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB.
That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM--something that no device has in the real world. Most viruses are very small.
This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

QUESTION 4
Refer to the web filter raw logs.



```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvdbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"

date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

A. Social networking web filter category is configured with the action set to authenticate.
B. The action on firewall policy ID 1 is set to warning.
C. Access to the social networking web filter category was explicitly blocked to all users.
D. The name of the firewall policy is all_users_web.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221#:~:text=Hard%20timeout%3A%20User%20

QUESTION 7
Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
B. To finish any inspection operations
C. To remove the NAT operation
D. To generate logs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

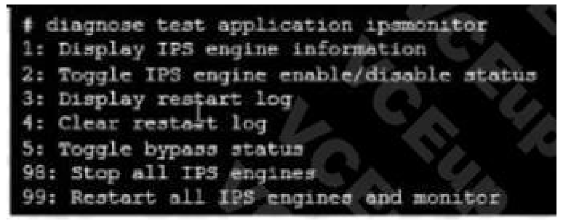
QUESTION 8
Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. SSH
B. HTTPS
C. FTM
D. FortiTelemetry

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.4.0/hardening-yourfortigate/995103/buildingsecurity-into-fortios

QUESTION 9
Refer to the exhibit.



```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.
Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.
B. The IPS engine was unable to prevent an intrusion attack .
C. The IPS engine was blocking all traffic.
D. The IPS engine will continue to run in a normal state.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpuusage

QUESTION 10
By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuardservers.
Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering?

A. set fortiguard-anycast disable
B. set webfilter-force-off disable
C. set webfilter-cache disable
D. set protocol tcp

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: y default, "fortiguard-anycast" is enabled, and this setting only works with "set protocol https". To use udp (ie. "set protocol udp"), "fortiguard-anycast" must be disabled.
Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=FD48294"
By default, FortiGate is configured to enforce the use of HTTPS port 443 to perform live filtering with FortiGuard or FortiManager. Other ports and protocols are available by disabling the FortiGuard anycast setting on the CLI."

QUESTION 11
How does FortiGate act when using SSL VPN in web mode?

A. FortiGate acts as an FDS server.
B. FortiGate acts as an HTTP reverse proxy.
C. FortiGate acts as DNS server.
D. FortiGate acts as router.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigatesslvpn-40-mr3.pdf

QUESTION 12

Which three statements explain a flow-based antivirus profile? (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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://forum .fortinet.com/tm .aspx?m=192309

QUESTION 13
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

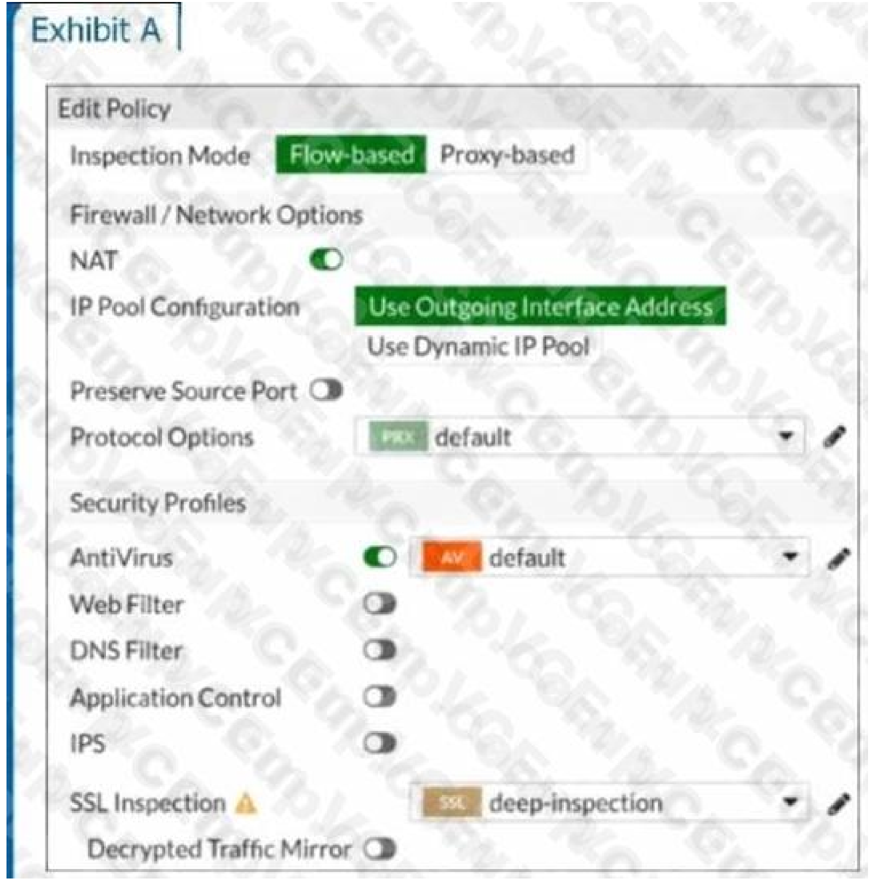


Exhibit A

Edit Policy

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●

IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve Source Port ○

Protocol Options: PRX default

Security Profiles

AntiVirus ● AV default

Web Filter ○

DNS Filter ○

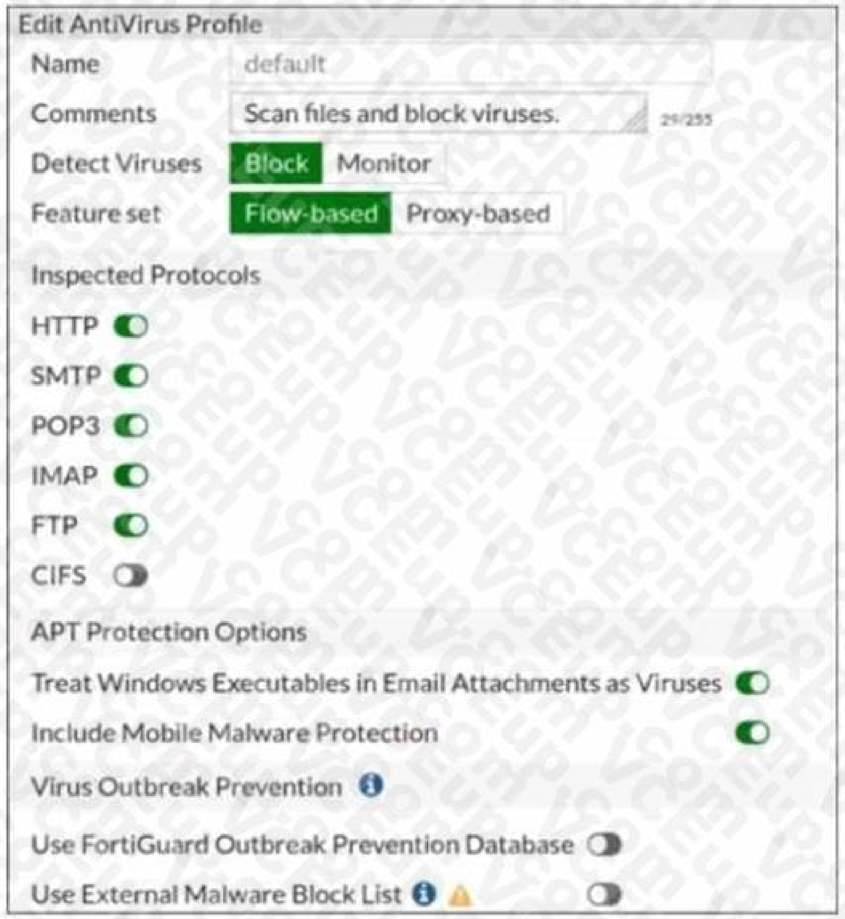
Application Control ○

IPS ○

SSL Inspection ⚠ SSL deep-inspection

Decrypted Traffic Mirror ○

Exhibit B



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Detect Viruses: [✓ Block] Monitor

Feature set: [✓ Flow-based] Proxy-based

Inspected Protocols

- HTTP ●
- SMTP ●
- POP3 ●
- IMAP ●
- FTP ●
- CIFS ○

APT Protection Options

- Treat Windows Executables in Email Attachments as Viruses ●
- Include Mobile Malware Protection ●

Virus Outbreak Prevention

- Use FortiGuard Outbreak Prevention Database ○
- Use External Malware Block List ○

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The firewall policy performs the full content inspection on the file.

B. The flow-based inspection is used, which resets the last packet to the user.

C. The volume of traffic being inspected is too high for this model of FortiGate.

D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
· "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately · When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

QUESTION 14
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Study Guide – IPsec VPN – IPsec configuration – Phase 1 Network.
When Dead Peer Detection (DPD) is enabled, DPD probes are sent to detect a failed tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to failover to a backup connection when the primary connection fails to keep the connectivity between the sites up.
There are three DPD modes. On demand is the default mode.
Study Guide – IPsec VPN – Redundant VPNs.
Add one phase 1 configuration for each tunnel. DPD should be enabled on both ends.
Add at least one phase 2 definition for each phase 1.
Add one static route for each path. Use distance or priority to select primary routes over backup routes (routes for the primary VPN must have a lower distance or lower priority than the backup).
Alternatively, use dynamic routing.
Configure FW policies for each IPsec interface.

QUESTION 15
Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Antivirus engine

B. Intrusion prevention system engine

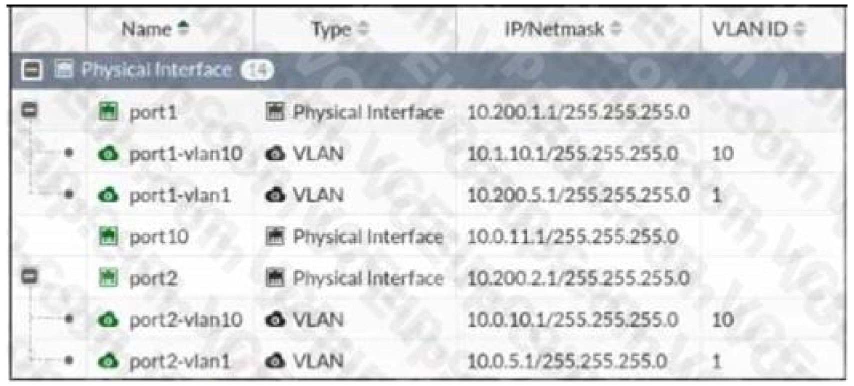
C. Flow engine

D. Detection engine

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control
Reference: http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/applicationcontrol

QUESTION 16
Refer to the exhibit.



Name	Type	IP/Netmask	VLAN ID
Physical Interface 14			
port1	Physical Interface	10.200.1.1/255.255.255.0	
port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
port10	Physical Interface	10.0.11.1/255.255.255.0	
port2	Physical Interface	10.200.2.1/255.255.255.0	
port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

A. Traffic between port2 and port2-vlan1 is allowed by default.

B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

C. port1 is a native VLAN.

D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

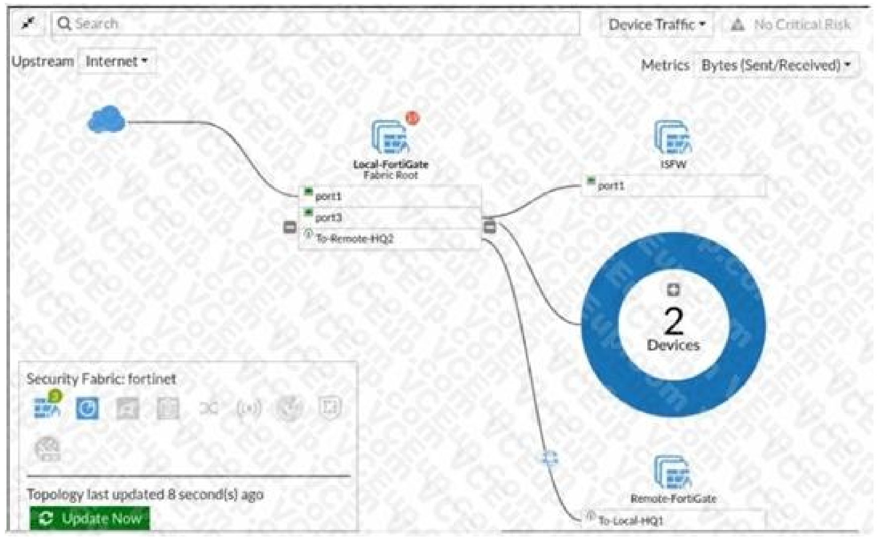
QUESTION 17
Which statement about video filtering on FortiGate is true?

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering

QUESTION 18
Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. There are five devices that are part of the security fabric.
B. Device detection is disabled on all FortiGate devices.
C. This security fabric topology is a logical topology view.
D. There are 19 security recommendations for the security fabric.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
References:
https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabrictopology

QUESTION 19
A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through

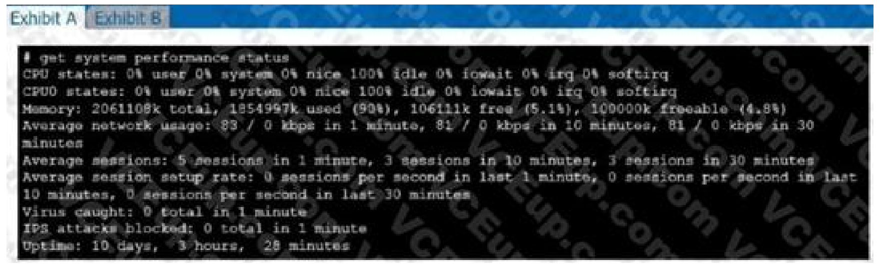
HTTPS, FortiGate does not detect the virus and the file can be downloaded.
What is the reason for the failed virus detection by FortiGate?

A. The website is exempted from SSL inspection.
B. The EICAR test file exceeds the protocol options oversize limit.
C. The selected SSL inspection profile has certificate inspection enabled.
D. The browser does not trust the FortiGate self-signed CA certificate.

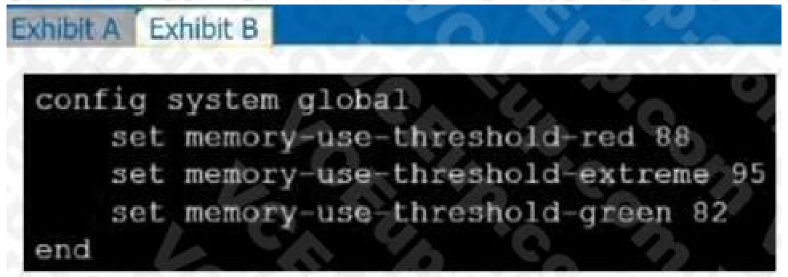
Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https traffic requires SSL decryption. Check the ssh inspection profile

QUESTION 20
Refer to the exhibits.



```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30
minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last
10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days,  3 hours,  28 minutes
```



```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

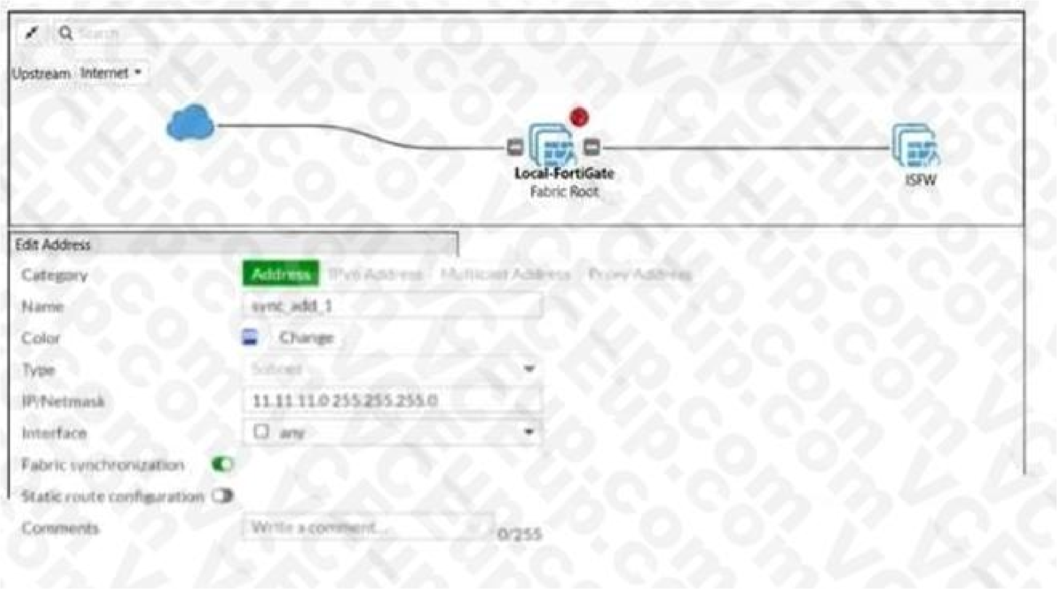
Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)

A. Administrators can access FortiGate only through the console port.
B. FortiGate has entered conserve mode.
C. FortiGate will start sending all files to FortiSandbox for inspection.
D. Administrators cannot change the configuration.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Conserve-mode-changes/tap/198502
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Conserve-mode-changes/ta-p/198502
configurable thresholds
Though it is recommended to keep the default memory threshold, a new CLI command has been added to allow administrators to adjust the thresholds.
Default values are :
- red : 88% of total memory is considered "used memory"
- extreme : 95% of total memory is considered "used memory"
- green : 82% of total memory is considered "used memory"

QUESTION 21
Refer to the exhibits.
Exhibit A.



Category: Address | IPv6 Address | Multicast Address | Proxy Address

Name: sync_add_1

Color: Change

Type: Subnet

IP/Netmask: 11.11.11.0 255.255.255.0

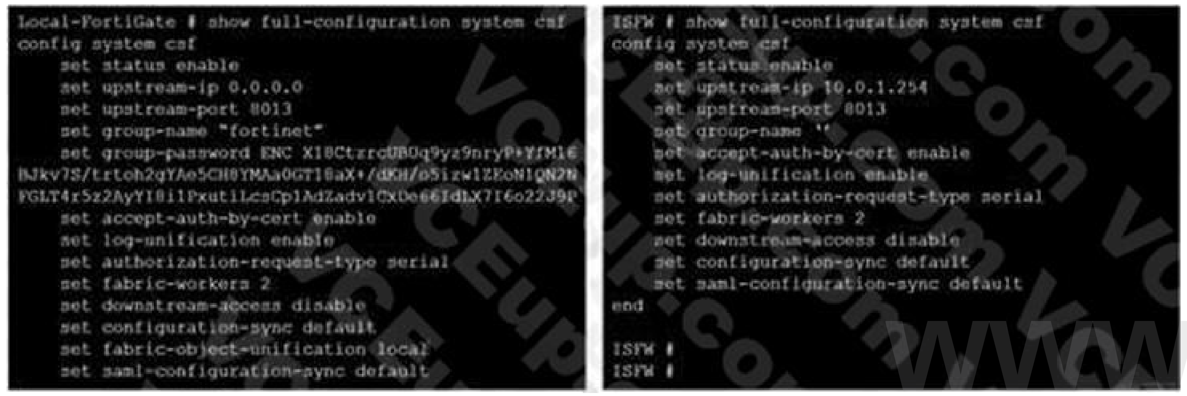
Interface: any

Fabric synchronization: ●

Static route configuration: ○

Comments: Write a comment... 0/255

Exhibit B.



```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 0.0.0.0
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC X18CtzrcUBOq9yz9nryP+YfM16
BJkv7S/trtoh2gYAe5CH0YMAa0GT18aX+/dKH/o5izw1ZEoN1QN2N
FGLT4r5z2AyY18i1PxutiLcsCp1AdZadv1CxDe66IdLX7I6o22J9P
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml-configuration-sync default
```

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 10.0.1.254
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync default
end

ISFW #
ISFW #
```

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).
What must the administrator do to synchronize the address object?

A. Change the csf setting on Local-FortiGate (root) to set configuration-sync local.
B. Change the csf setting on ISFW (downstream) to set configuration-sync local.
C. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.
D. Change the csf setting on ISFW (downstream) to set fabric-object-unification default.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.4.5/administrationguide/880913/synchronizing-objects-across-the-security-fabric

QUESTION 22
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.
D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspectionmode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

QUESTION 23
Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

A. The security actions applied on the web applications will also be explicitly applied on the thirdparty websites.
B. The application signature database inspects traffic only from the original web application server.
C. FortiGuard maintains only one signature of each web application that is unique.
D. FortiGate can inspect sub-application traffic regardless where it was originated.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:
https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPXAdminGuide/300_System/303d_FortiG

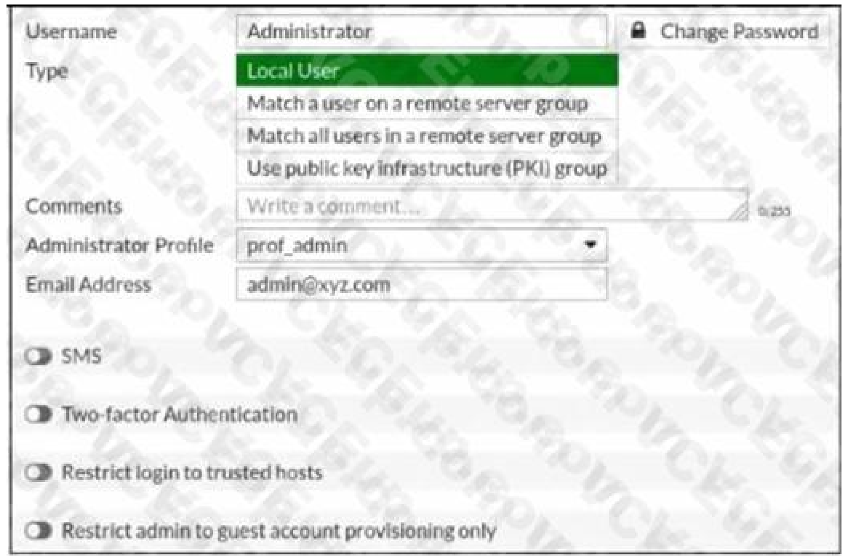
QUESTION 24
An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
Which DPD mode on FortiGate will meet the above requirement?

A. Disabled
B. On Demand
C. Enabled
D. On Idle

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=FD40813

QUESTION 25
Refer to the exhibit.



Username: Administrator
🔒 Change Password
Type: Local User
Match a user on a remote server group
Match all users in a remote server group
Use public key infrastructure (PKI) group
Comments: Write a comment... 0/255
Administrator Profile: prof_admin
Email Address: admin@xyz.com
○ SMS
○ Two-factor Authentication
○ Restrict login to trusted hosts
○ Restrict admin to guest account provisioning only

The global settings on a FortiGate device must be changed to align with company security policies.

What does the Administrator account need to access the FortiGate global settings?

A. Change password
B. Enable restrict access to trusted hosts
C. Change Administrator profile
D. Enable two-factor authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=FD34502

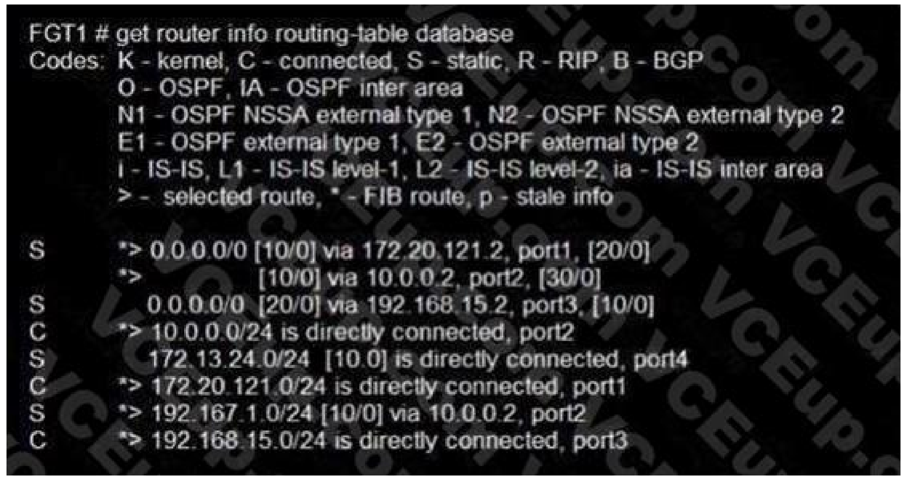
QUESTION 26
Which two statements are correct about SLA targets? (Choose two.)

A. You can configure only two SLA targets per one Performance SLA.
B. SLA targets are optional.
C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
D. SLA targets are used only when referenced by an SD-WAN rule.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-slasla-targets

QUESTION 27
Refer to the exhibit.



```
FGT1 # get router info routing-table database
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        > -  selected route, * - FIB route, p - stale info

S       *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
        *>           [10/0] via 10.0.0.2, port2, [30/0]
S          0.0.0.0/0  [20/0] via 192.168.15.2, port3, [10/0]
C       *> 10.0.0.0/24 is directly connected, port2
S          172.13.24.0/24  [10.0] is directly connected, port4
C       *> 172.20.121.0/24 is directly connected, port1
S       *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C       *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

A. The port3 default route has the highest distance.
B. The port3 default route has the lowest metric.
C. There will be eight routes active in the routing table.
D. The port1 and port2 default routes are active in the routing table.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

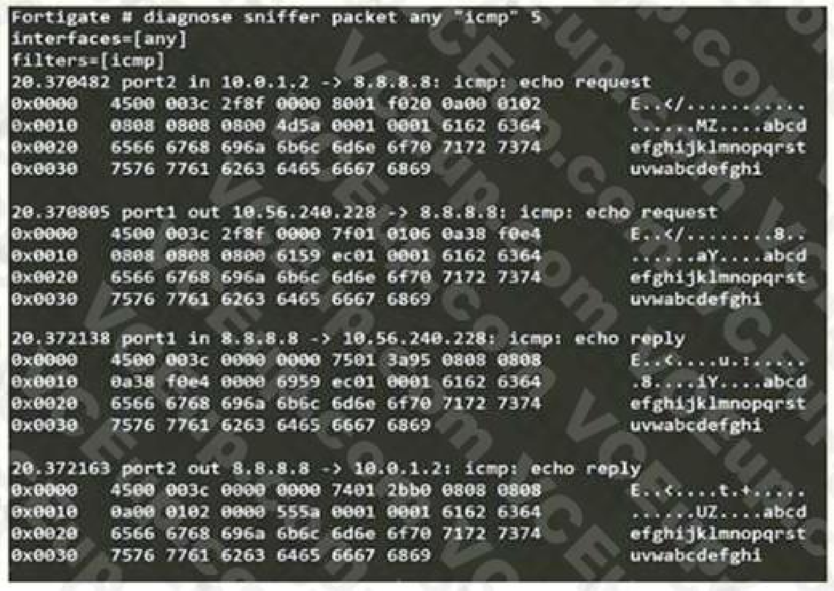
QUESTION 28
When configuring a firewall virtual wire pair policy, which following statement is true?

A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
B. Only a single virtual wire pair can be included in each policy.
C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
D. Exactly two virtual wire pairs need to be included in each policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=FD48690

QUESTION 29
Refer to the exhibit.



```
Fortigate # diagnose sniffer packet any "icmp" 5
interfaces=[any]
filters=[icmp]
20.370482 port2 in 10.0.1.2 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 8001 f020 0a00 0102        E..</...........
0x0010   0808 0808 0800 4d5a 0001 0001 6162 6364        ......MZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.370805 port1 out 10.56.240.228 -> 8.8.8.8: icmp: echo request
0x0000   4500 003c 2f8f 0000 7f01 0106 0a38 f0e4        E..</........8..
0x0010   0808 0808 0800 6159 ec01 0001 6162 6364        ......aY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372138 port1 in 8.8.8.8 -> 10.56.240.228: icmp: echo reply
0x0000   4500 003c 0000 0000 7501 3a95 0808 0808        E..<....u.:.....
0x0010   0a38 f0e4 0000 6959 ec01 0001 6162 6364        .8....iY....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi

20.372163 port2 out 8.8.8.8 -> 10.0.1.2: icmp: echo reply
0x0000   4500 003c 0000 0000 7401 2bb0 0808 0808        E..<....t.+.....
0x0010   0a00 0102 0000 555a 0001 0001 6162 6364        ......UZ....abcd
0x0020   6566 6768 696a 6b6c 6d6e 6f70 7172 7374        efghijklmnopqrst
0x0030   7576 7761 6263 6465 6667 6869                  uvwabcdefghi
```

An administrator is running a sniffer command as shown in the exhibit.
Which three pieces of information are included in the sniffer output? (Choose three.)

A. Interface name
B. Ethernet header
C. IP header
D. Application header
E. Packet payload

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://kb.fortinet.com/kb/documentLink .do?externalID=11186Study Guide – Routing – Diagnostics – Packet Capture Verbosity Level.
# diagnose sniffer packet <interface> ‘<filter>’ <verbosity> <count> <timestamp> <frame size> In the example, verbosity is 5.
The verbosity level specifies how much info you want to display.
1 (default): IP Headers.
2: IP Headers, Packet Payload.

3. IP Headers, Packet Payload, Ethernet Headers.
4: IP Headers, Interface Name.
5: IP Headers, Packet Payload, Interface Name.
6: IP Headers, Packet Payload, Ethernet Headers, Interface Name.

QUESTION 30
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).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference: https://community.fortinet.com/t5/Support-Forum/Collector-Agent-and-problemgetting-login-info/m-p/95481