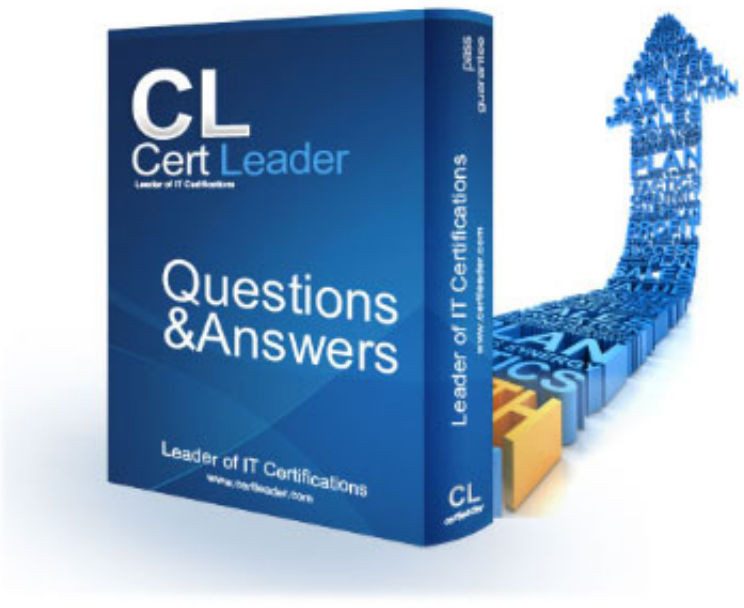
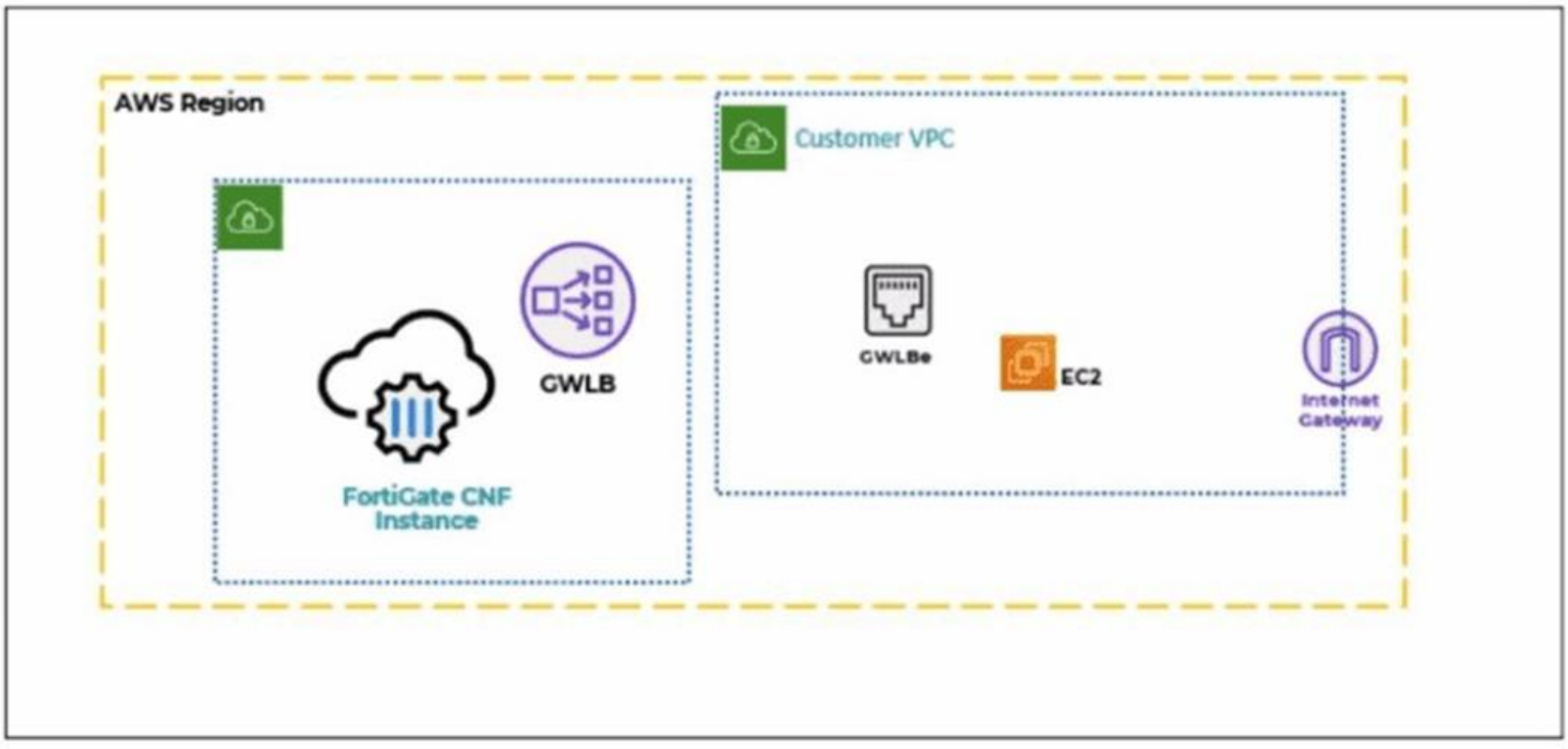
NSE4_FGT_AD-7.6 Dumps

Fortinet NSE 4 - FortiOS 7.6 Administrator

https://www.certleader.com/NSE4_FGT_AD-7.6-dumps.html



NEW QUESTION 1
Refer to the exhibit.
A partial cloud topology is shown.



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.
During the deployment, which components must the FortiGate CNF create to handle traffic from the EC2 instance?

A. The customer VPC and GWLBe
B. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)
C. The CNF VP
D. customer VP
E. and GWLB
F. The GWL
G. GWLBe, and the internet gateway (IGW) in the customer VPC

Answer: B

NEW QUESTION 2
Refer to the exhibit.

FortiGate SD-WAN zone configuration

An SD-WAN zone configuration on the FortiGate GUI is shown. Based on the exhibit, which statement is true?

A. The Underlay zone contains no member.
B. The virtual-wan-link and overlay zones can be deleted
C. The Underlay zone is the zone by default.
D. port2 and port3 are not assigned to a zone.

Answer: A

NEW QUESTION 3
Refer to the exhibit showing a debug flow output.

Debug Flow output

```
vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4. type=8, code=0, id=3, seq=5.
allocate a new session-00000721
in-[port4], out-[]
len=0
result: skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
find a route: flag=00000000 gw-0.0.0.0 via port2
in-[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0
gnum-100004, use addr/intf hash, len=3
checked gnum-100004 policy-2, ret-matched, act-accept
ret-matched
gnum-4e20, check-ffffffffa002c9c7
checked gnum-4e20 policy-6, ret-no-match, act-accept
gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000
policy-2 is matched, act-drop
after iprope_captive_check(): is_captive-0, ret-matched, act-drop, idx-2
Denied by forward policy check (policy 2)
```

Which two conclusions can you make from the debug flow output? (Choose two answers)

A. The default gateway is configured on port2.
B. The RPF check fails.
C. The debug flow is for UDP traffic.
D. The matching firewall policy denies the traffic.

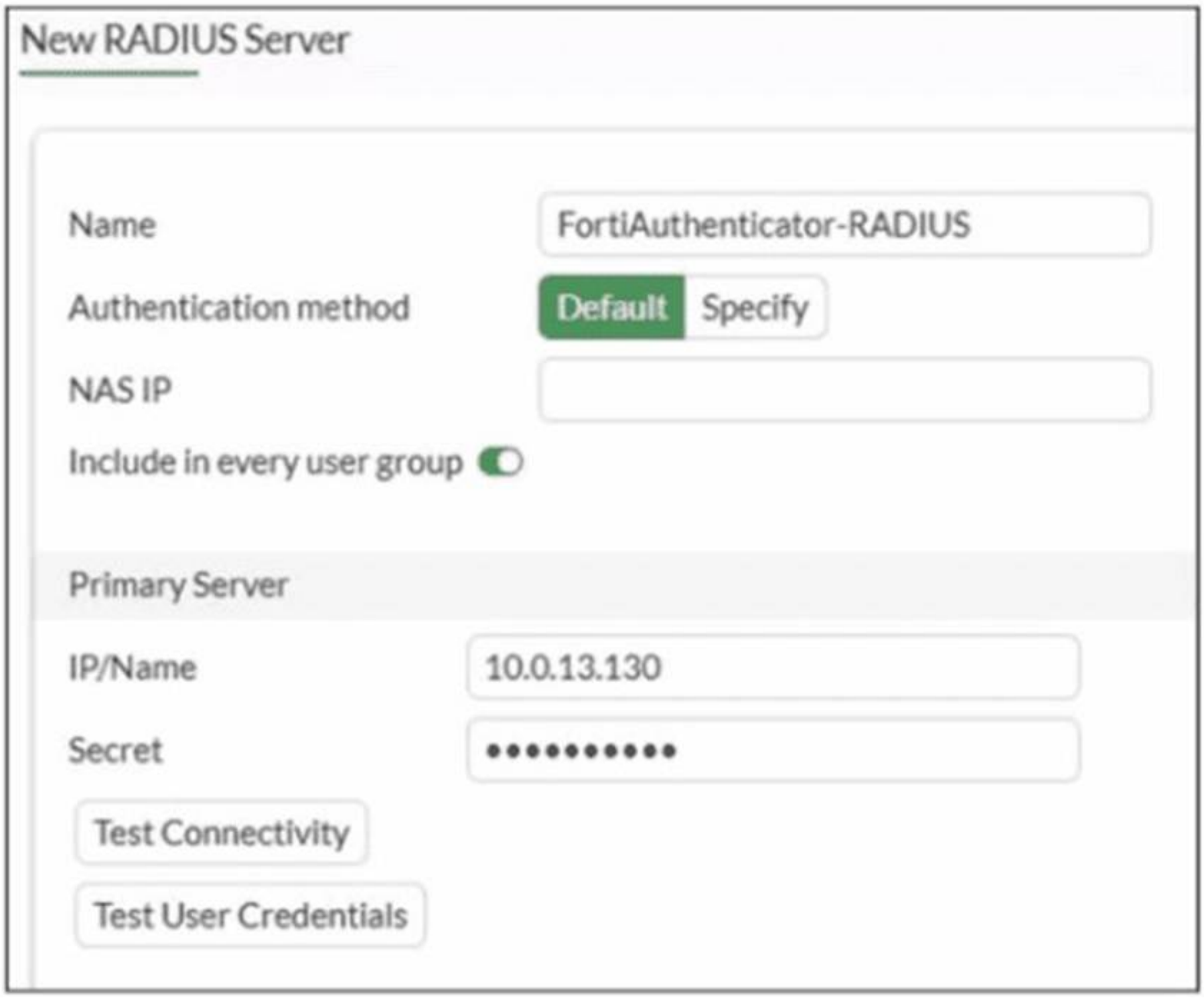
Answer: AD

NEW QUESTION 4
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 there is no inbound traffic.
Which DPD mode on FortiGate meets this requirement?

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

Answer: A

NEW QUESTION 5
Refer to the exhibit.
A RADIUS server configuration is shown.



An administrator added a configuration for a new RADIUS server While configuring, the administrator enabled Include in every user group What is the impact of enabling Include in every user group in a RADIUS configuration?

A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
C. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.
D. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.

Answer: A

NEW QUESTION 6
An administrator manages a FortiGate model that supports NTurbo How does NTurbo acceleration enhance antivirus performance?

A. For flow-based inspectio
B. NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.
C. For flow-based inspectio
D. NTurbo creates two inspection sessions on the FortiGate device.
E. For proxy-based inspectio
F. NTurbo offloads traffic to the content processor.
G. For proxy-based inspectio
H. NTurbo buffers the whole file and then sends it to the antivirus engine.

Answer: A

NEW QUESTION 7
Which two statements describe characteristics of automation stitches? (Choose two answers)

A. Actions involve only devices included in the Security Fabric.
B. An automation stitch can have multiple triggers.
C. Multiple actions can run in parallel.
D. Triggers can involve external connectors.

Answer: CD

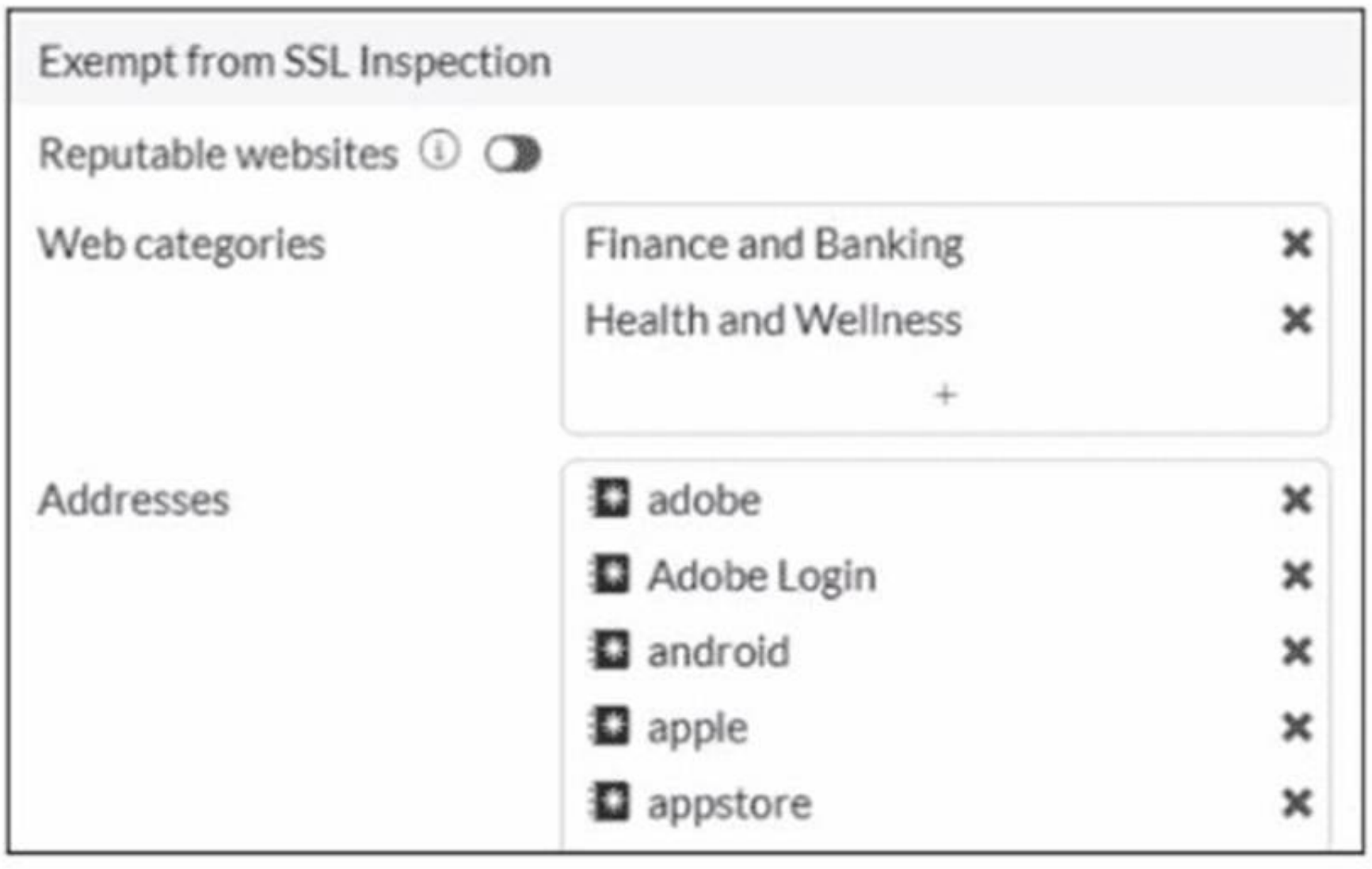
NEW QUESTION 8
FortiGate is integrated with FortiAnalyzer and FortiManager.

When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

A. Universally Unique Identifier
B. Policy ID
C. Sequence ID
D. Log ID

Answer: A

NEW QUESTION 9
Refer to the exhibit.



The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit For which two reasons are these web categories exempted? (Choose two.)

A. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
B. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.
C. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
D. The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.

Answer: BC

NEW QUESTION 10
Which three statements explain a flow-based antivirus profile? (Choose three answers)

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

Answer: ABD

NEW QUESTION 10
An administrator wanted to configure an IPS sensor to block traffic that triggers the signature set number of times during a specific time period. How can the administrator achieve the objective?

A. Use IPS group signatures, set rate-mode 60.
B. Use IPS packet logging option with periodical filter option.
C. Use IPS signatures, rate-mode periodical option.
D. Use IPS filter, rate-mode periodical option.

Answer: D

NEW QUESTION 12
You have created a web filter profile named restrictmedia-profile with a daily category usage quota.

When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down.
What could be the reason?

A. The web filter profile is already referenced in another firewall policy.
B. The firewall policy is in no-inspection mode instead of deep-inspection.
C. The naming convention used in the web filter profile is restricting it in the firewall policy.
D. The inspection mode in the firewall policy is not matching with web filter profile feature set.

Answer: D

NEW QUESTION 14
Refer to the exhibits.

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87  kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions  in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions  in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32  kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions    in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions  in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds.
Which FortiGate is the primary?

A. HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting
B. HQ-NGFW-2 with the parameter priority setting
C. HQ-NGFW-1 with the parameter override setting
D. HQ-NGFW-2 with the parameter memory-failover-threshold setting

Answer: D

NEW QUESTION 18
Refer to the exhibit.

SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	✔ Accept (8.08 kB / 27...	1 (DIA)	port2		
YouTube	✔ Accept (UTM Allowed)	1 (DIA)	port2		
Facebook	✔ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✔ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✔ Accept (3.33 kB / 10...	1 (DIA)	port1		
YouTube	✔ Accept (44.63 kB / 3....	1 (DIA)	port2		
CNN	✔ Accept (UTM Allowed)	1 (DIA)	port1		
CNN	✔ Accept (UTM Allowed)	1 (DIA)	port2		
CNN	✔ Accept (UTM Allowed)	1 (DIA)	port2		

The administrator configured SD-WAN rules and set the FortiGate traffic log page to display SD-WAN-specific columns: SD-WAN Quality and SD-WAN Rule Name
FortiGate allows the traffic according to policy ID 1 placed at the top. This is the policy that allows SD-WAN traffic. Despite these settings, the traffic logs do not show the name of the SD-WAN rule used to steer those traffic flows
What could be the reason?

A. SD-WAN rule names do not appear immediatel
B. The administrator must refresh the page.
C. There is no application control profile applied to the firewall policy.
D. Destinations in the SD-WAN rules are configured for each application, but feature visibility is not enabled.
E. FortiGate load balanced the traffic according to the implicit SD-WAN rule.

Answer: D

NEW QUESTION 21
Which two statements are correct when the FortiGate device enters conserve mode? (Choose two.)

A. FortiGate refuses to accept configuration changes.
B. FortiGate halts complete system operation and requires a reboot to regain available resources.
C. FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.
D. FortiGate continues to run critical security actions, such as quarantine.

Answer: AC

NEW QUESTION 22
When configuring firewall policies which of the following is true regarding the policy ID? (Choose two.)

A. A firewall policy ID identifies the order of policy execution in firewall policies.
B. A policy ID cannot be modified once a policy is created.
C. You can create a policy in CLI with policy ID 0
D. It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.

Answer: BC

NEW QUESTION 24
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

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

* One year free update

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

* Trusted by Millions

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

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4_FGT_AD-7.6 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT_AD-7.6-dumps.html