PASS QUESTION

QUESTION & ANSWER

HIGHER QUALITY, BETTER SERVICE

Exam : **NSE4_FGT-7.2**

Title : Fortinet NSE 4 - FortiOS 7.2

Version : DEMO

1.Refer to the exhibit.

```
1: date=2020-08-14 time=06:28:24 logid= "0316013056" type= "utm" subtype= "webfilter"
eventtype= "ftgd_blk" level= "warning" vd= "root" eventtime= 1597343304867252750
policyid=2 sessionid=83212 srcip=10.0.1.10 srcport=53742 srcintf= "port3" srci ntfrole=
"undefined" dstip=159.65.216.232 dstport=443 dstintf= "port1" dstintfrole= "wan" proto=6
service= "HTTPS" hostname= "etp-experiment-1.dummytracker.org" profile= "default"
action= "blocked" reqtype= "direct" url= "https://etp-experiment-1.dumytracker.org/"
sentbyte=517 rcvdbyte=0 direction= "outgoing" msg= "URL belongs to a denied category in
policy" method= "domain" cat=26 catdesc= "Malicious Websites" crscore=30 craction=
4194304 crlevel= "high"
```

Based on the raw log, which two statements are correct? (Choose two.)

A. Traffic is blocked because Action is set to DENY in the firewall policy.

B. Traffic belongs to the root VDOM.

C. This is a security log.

D. Log severity is set to error on FortiGate.

Answer: B,C

2.Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.

B. ADVPN is only supported with IKEv2.

C. Tunnels are negotiated dynamically between spokes.

D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: A,C

3.Refer to the exhibit.

```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
     pingsvr_flip_timeout/expire=3600s/2781s
     'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
     'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.

B. FortiGate devices are not in sync because one device is down.

C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.

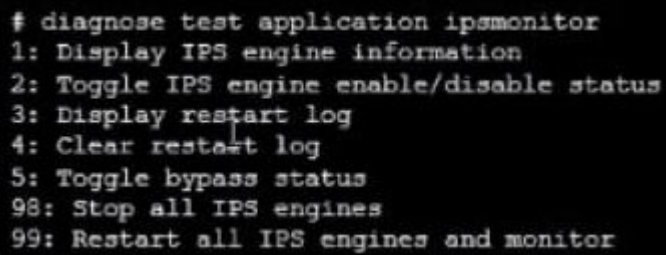D. FortiGate SN FGVM010000064692 has the higher HA priority.

Answer: A,D

Explanation:

1. Override is disable by default - OK

2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary" The QUESTION NO: here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide. https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-

override-disab

4.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.
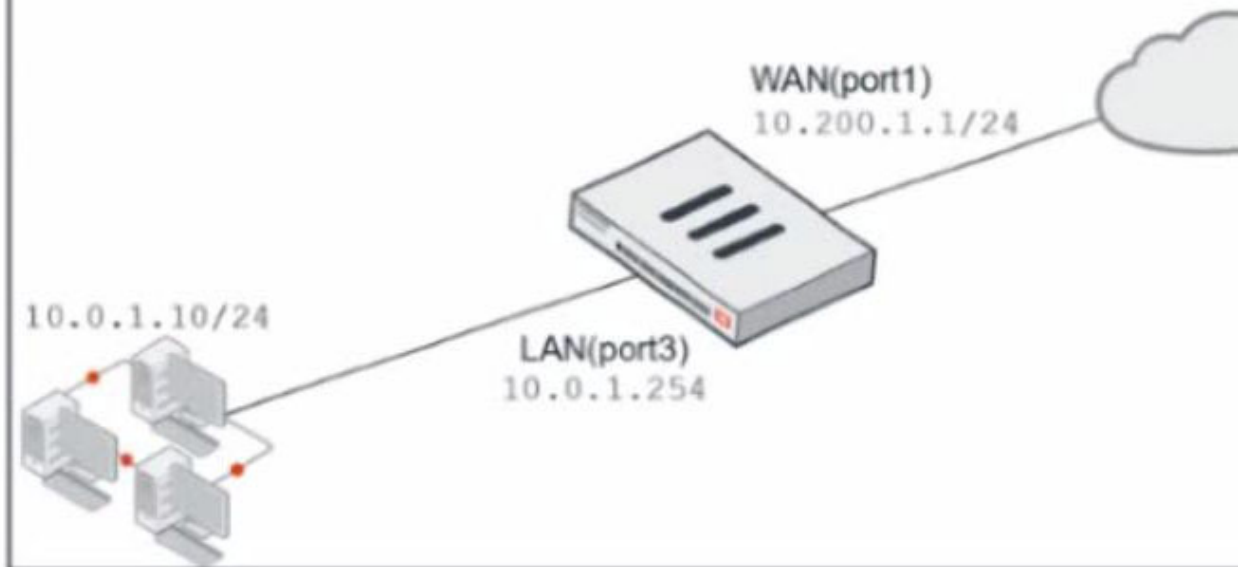
D. The IPS engine will continue to run in a normal state.

Answer: A

Explanation:

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

5.Refer to the exhibit.

Network diagram

WAN(port1)
10.200.1.1/24

10.0.1.10/24

LAN(port3)
10.0.1.254

Virtual IP

VIP type	IPv4	
Name	VIP	
Comments	Write a comment...	0/255
Color	Change	

IP Poc

| Name |
| Comment |
| Type |
| External II |

The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration.

The WAN (port1) interface has the IP address 10.200. 1. 1/24.

The LAN (port3) interface has the IP address 10 .0.1.254. /24.

The first firewall policy has NAT enabled using IP Pool.

The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

A. 10.200.1.1

B. 10.200.3.1

C. 10.200.1.100

D. 10.200.1.10

Answer: C

Explanation:

Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.