Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

NEW QUESTION 1
- (Exam Topic 1)
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

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.

Answer: B

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.

NEW QUESTION 2
- (Exam Topic 1)
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

Answer: BCE

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview

NEW QUESTION 3
- (Exam Topic 1)
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

Answer: CD

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 inspection-mode 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

NEW QUESTION 4
- (Exam Topic 1)
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.

Answer: BC

Explanation:
B - because the customer requires the tunnels to notify when a tunnel goes down. DPD is designed for that purpose. To send a packet over a firewall to determine a failover for the next tunnel after a specific amount of time of not receiving a response from its peer.
C - remember when it comes to choosing a route with regards to Administrative Distance. The route with the lowest distance for that particular route will be chosen. So, by configuring a lower routing distance on the primary tunnel, means that the primary tunnel will be chosen to route packets towards their destination.

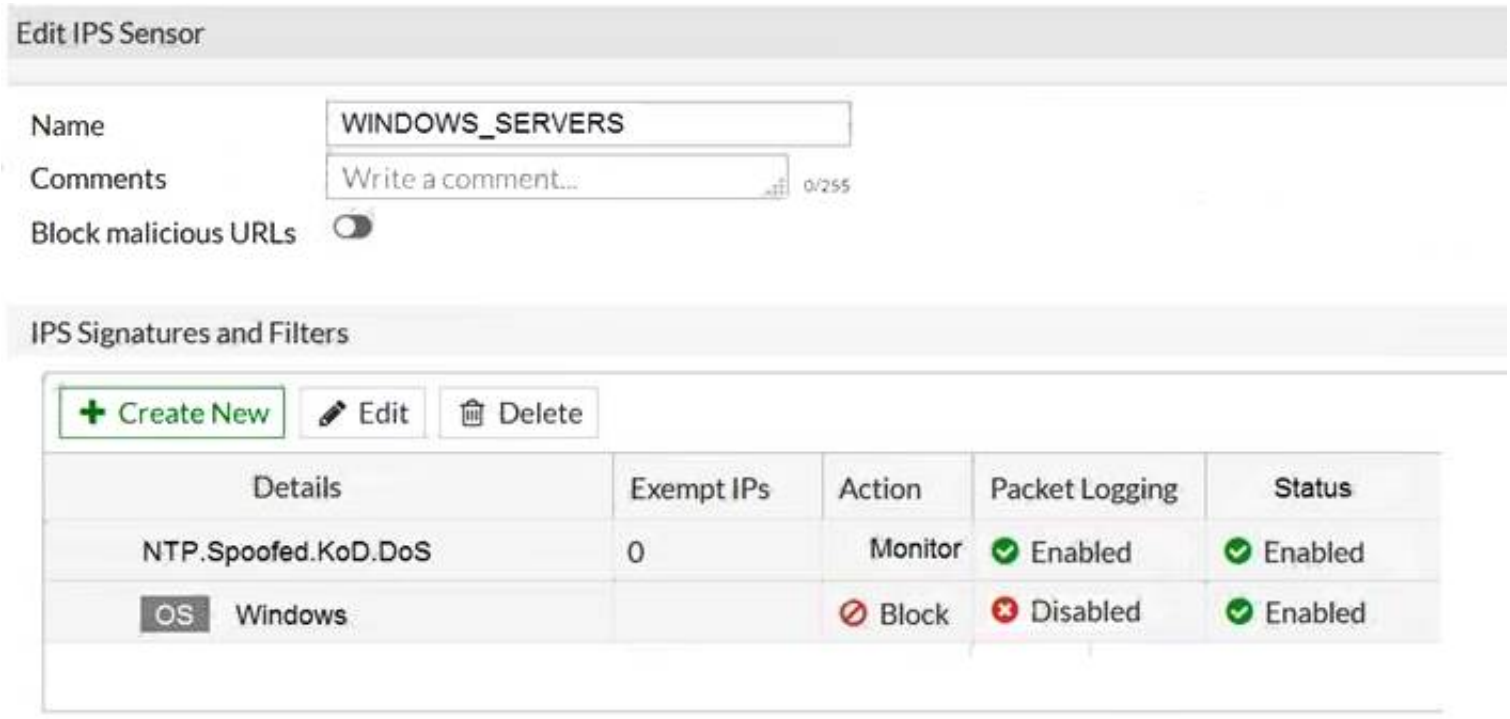
NEW QUESTION 5
- (Exam Topic 1)
Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

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.

Answer: BD

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

NEW QUESTION 6
- (Exam Topic 1)
Refer to the exhibit.



The exhibit shows the IPS sensor configuration.
If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will allow attackers matching the NTP.Spoofed.KoD.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 7
- (Exam Topic 1)
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.

Answer: AD

NEW QUESTION 8
- (Exam Topic 1)
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.

Answer: B

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

NEW QUESTION 9
- (Exam Topic 1)
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

Answer: B

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

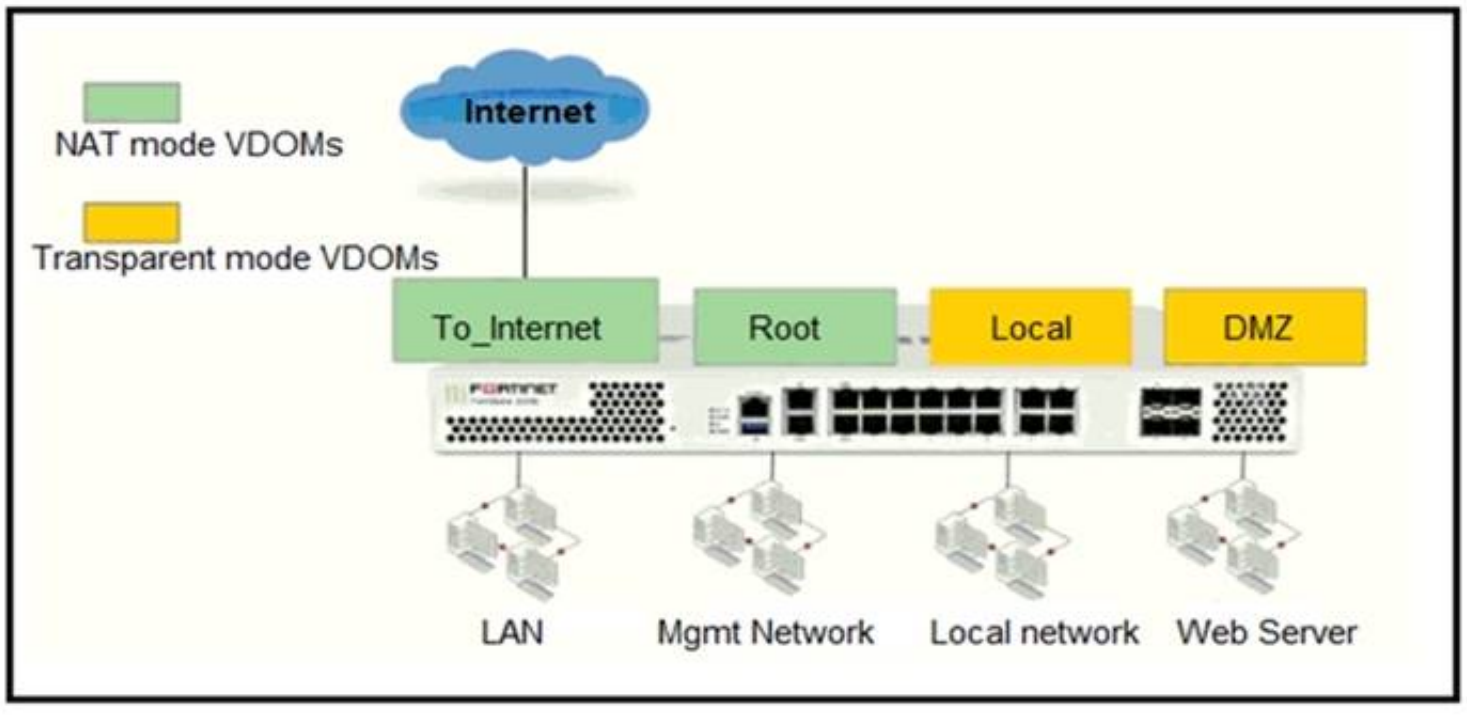
NEW QUESTION 10
- (Exam Topic 1)
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

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

Answer: D

Explanation:
"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

NEW QUESTION 10
- (Exam Topic 1)
Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
With this configuration, which statement is true?

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: A

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542

NEW QUESTION 14
- (Exam Topic 1)
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.

Answer: A

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

NEW QUESTION 18
- (Exam Topic 1)
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

Answer: BC

Explanation:
FortiGate_Security_6.4 page 384
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names— "no URLs or wildcard characters are allowed".

NEW QUESTION 22
- (Exam Topic 1)
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.

Answer: BD

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

NEW QUESTION 26
- (Exam Topic 1)
Which statement about the policy ID number of a firewall policy is true?

A. It is required to modify a firewall policy using the CLI.
B. It represents the number of objects used in the firewall policy.
C. It changes when firewall policies are reordered.
D. It defines the order in which rules are processed.

Answer: A

NEW QUESTION 30
- (Exam Topic 1)
Refer to the exhibits.

Exhibit A

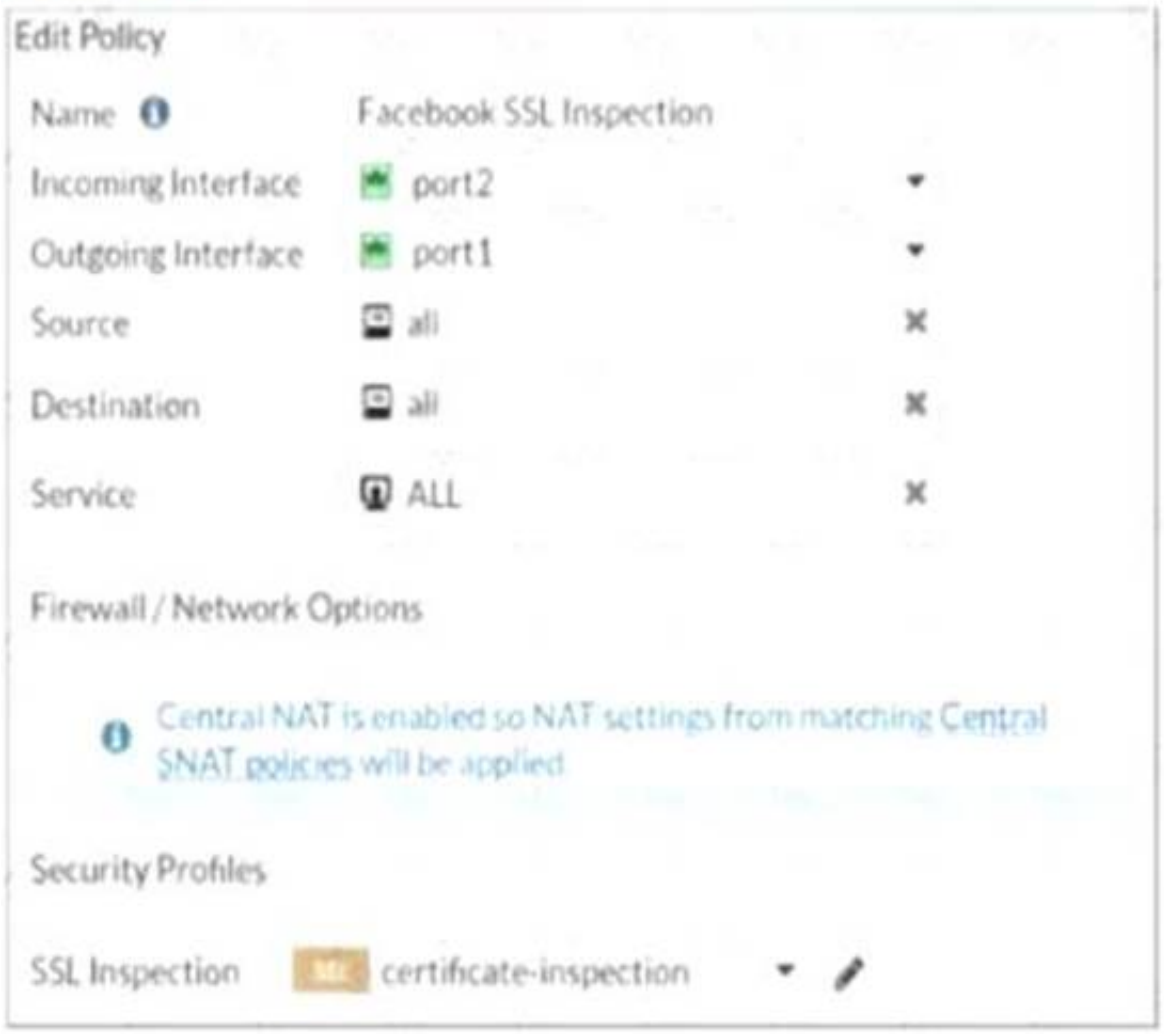


Exhibit B

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) tor Facebook.
Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.
Which part of the policy configuration must you change to resolve the issue?

A. The SSL inspection needs to be a deep content inspection.
B. Force access to Facebook using the HTTP service.
C. Additional application signatures are required to add to the security policy.
D. Add Facebook in the URL category in the security policy.

Answer: A

Explanation:
The lock logo behind Facebook_like.Button indicates that SSL Deep Inspection is Required.

NEW QUESTION 32
- (Exam Topic 1)
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
```

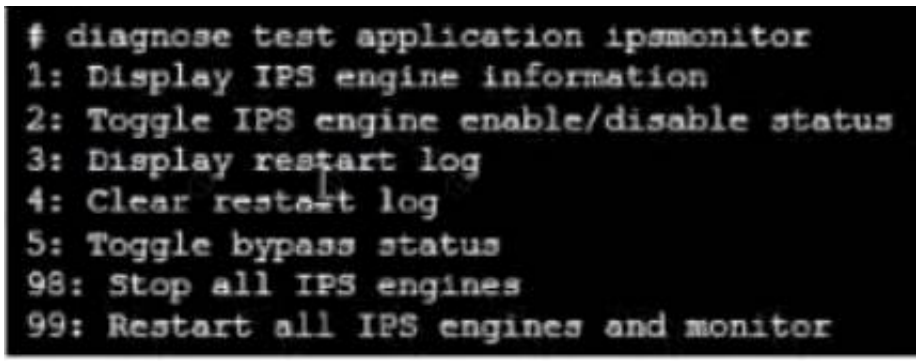
The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

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: AD

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 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

NEW QUESTION 33
- (Exam Topic 1)
Refer to the exhibit.



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

NEW QUESTION 37
- (Exam Topic 1)
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.

Answer: CD

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

NEW QUESTION 40
- (Exam Topic 2)
View the exhibit:

Status	Name	VLAN ID	Type	IP/Netmask
Physical(12)				
	port1		Physical Interface	10.200.1.1 255.255.255.0
	port1-VLAN1	1	VLAN	10.200.5.1 255.255.255.0
	port1-VLAN10	10	VLAN	10.0.10.1 255.255.255.0
	port2		Physical Interface	10.200.2.1 255.255.255.0
	port2-VLAN1	1	VLAN	10.0.5.1 255.255.255.0
	port2-VLAN10	10	VLAN	10.0.20.254 255.255.255.0
	port3		Physical Interface	10.0.1.254 255.255.255.0

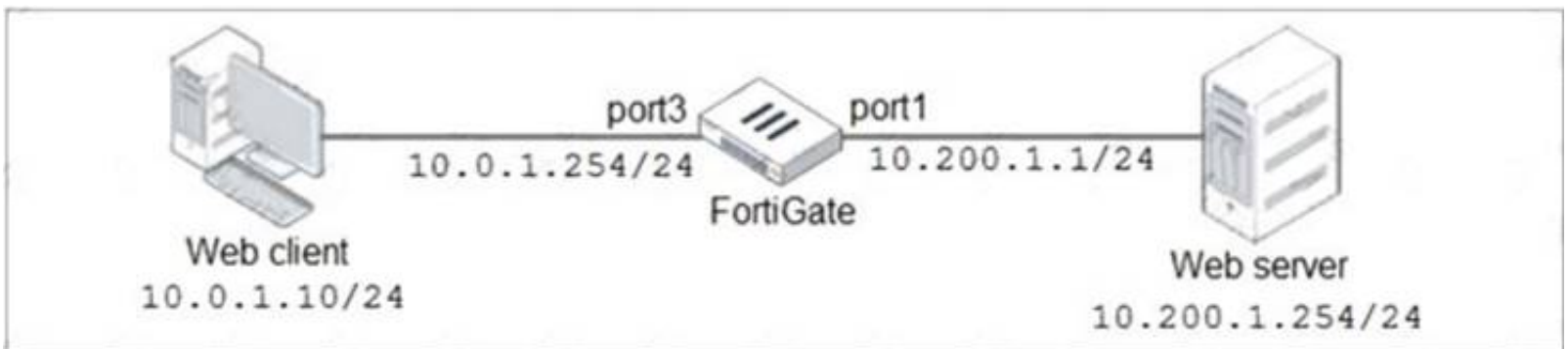
Which the FortiGate handle web proxy traffic rue? (Choose two.)

A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.

B. port-VLAN1 is the native VLAN for the port1 physical interface.
C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: AC

NEW QUESTION 41
- (Exam Topic 2)
Refer to the exhibit.




```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
```

In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10"
D. Execute a debug flow.

Answer: D

NEW QUESTION 44
- (Exam Topic 2)
Examine this PAC file configuration.

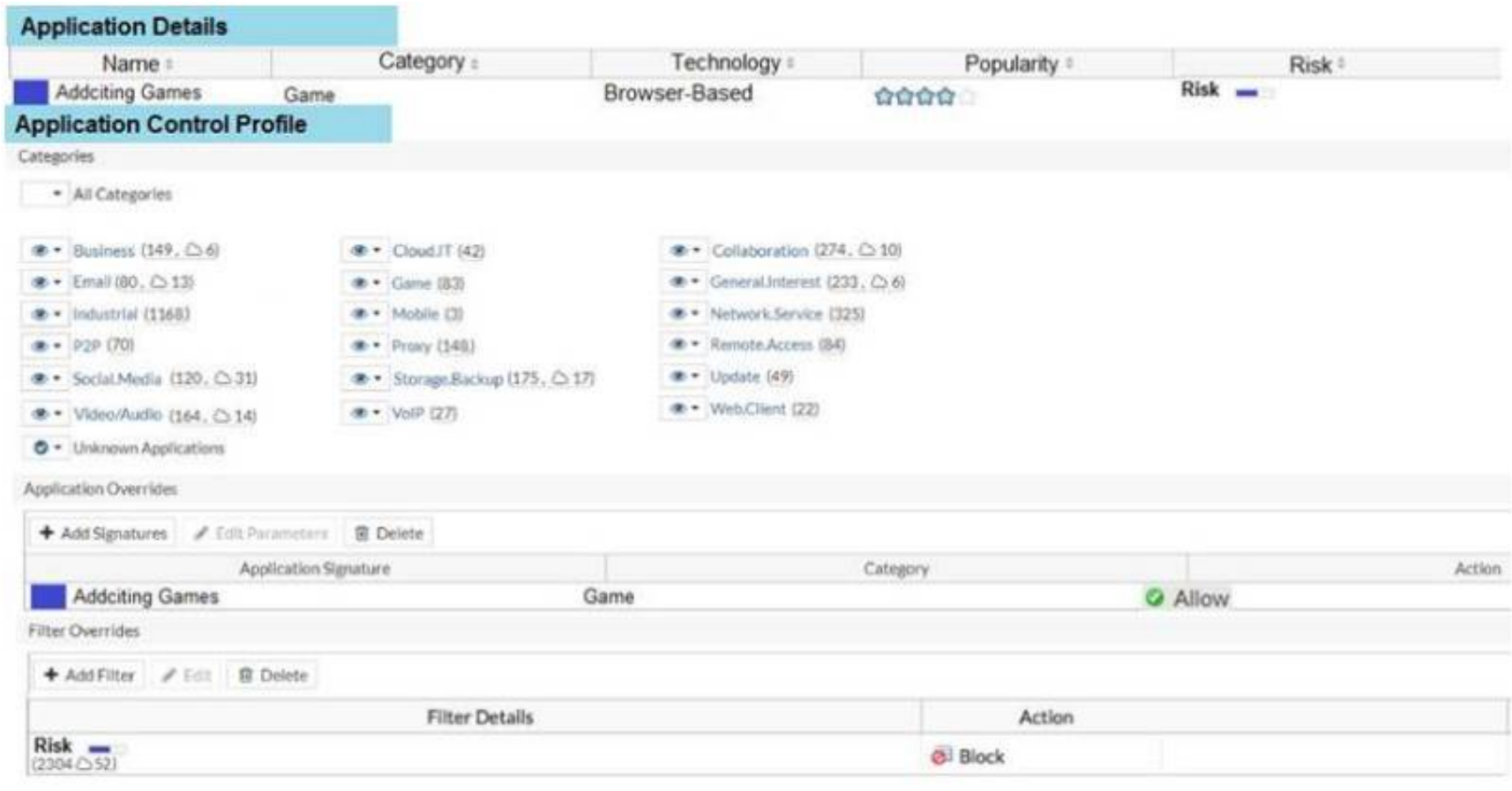
```
function FindProxyForURL (url, host) {
 if (shExpMatch (url, "*.fortinet.com/*")) {
    return "DIRECT";}
 if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
    return "PROXY" altproxy.corp.com: 8060";}
 return "PROXY proxy.corp.com: 8090";
}
```

Which of the following statements are true? (Choose two.)

A. Browsers can be configured to retrieve this PAC file from the FortiGate.
B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.
C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.
D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 47
- (Exam Topic 2)
View the exhibit.



A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting Games). Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.
B. Addicting.Games is blocked on the Filter Overrides configuration.
C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
D. Addcting.Games is allowed based on the Categories configuration.

Answer: A

NEW QUESTION 48
- (Exam Topic 2)
In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration? (Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.
B. The Incoming Interfac
C. Outgoing Interfac
D. Schedule, and Service fields can be shared with both IPv4 and IPv6.
E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
F. The IP version of the sources and destinations in a policy must match.
G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: BDE

NEW QUESTION 51
- (Exam Topic 2)
When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

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

Answer: B

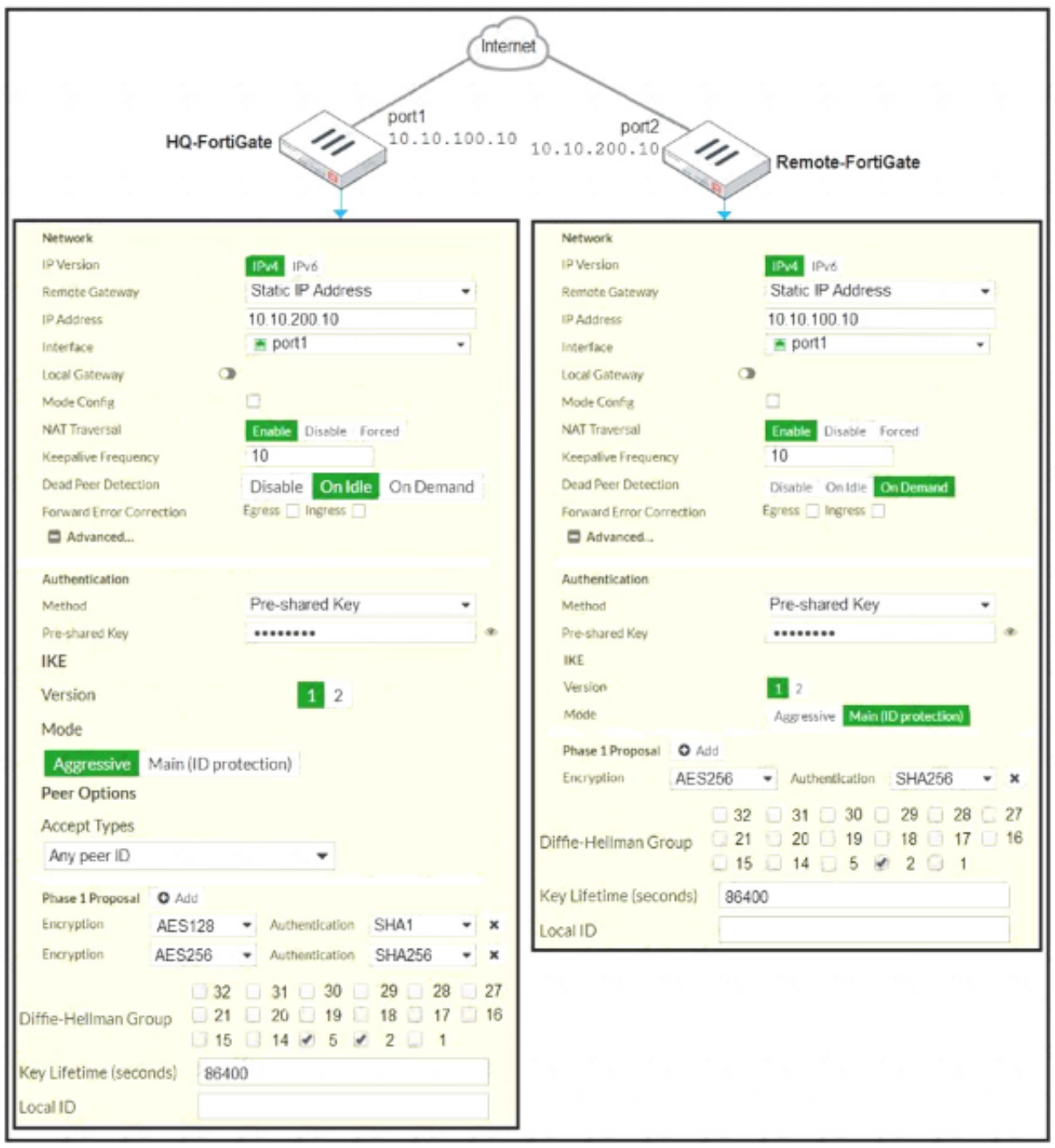
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies

NEW QUESTION 54
- (Exam Topic 2)
Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode
B. Can act as a Layer 2 switch as well as a Layer 3 router
C. All interfaces in the software switch share the same IP address
D. It can group only physical interfaces

Answer: AC

NEW QUESTION 56
- (Exam Topic 2)
Refer to the exhibit.



A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.
Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

A. On HQ-FortiGate, set IKE mode to Main (ID protection).
B. On both FortiGate devices, set Dead Peer Detection to On Demand.
C. On HQ-FortiGate, disable Diffie-Helman group 2.
D. On Remote-FortiGate, set port2 as Interface.

Answer: AD

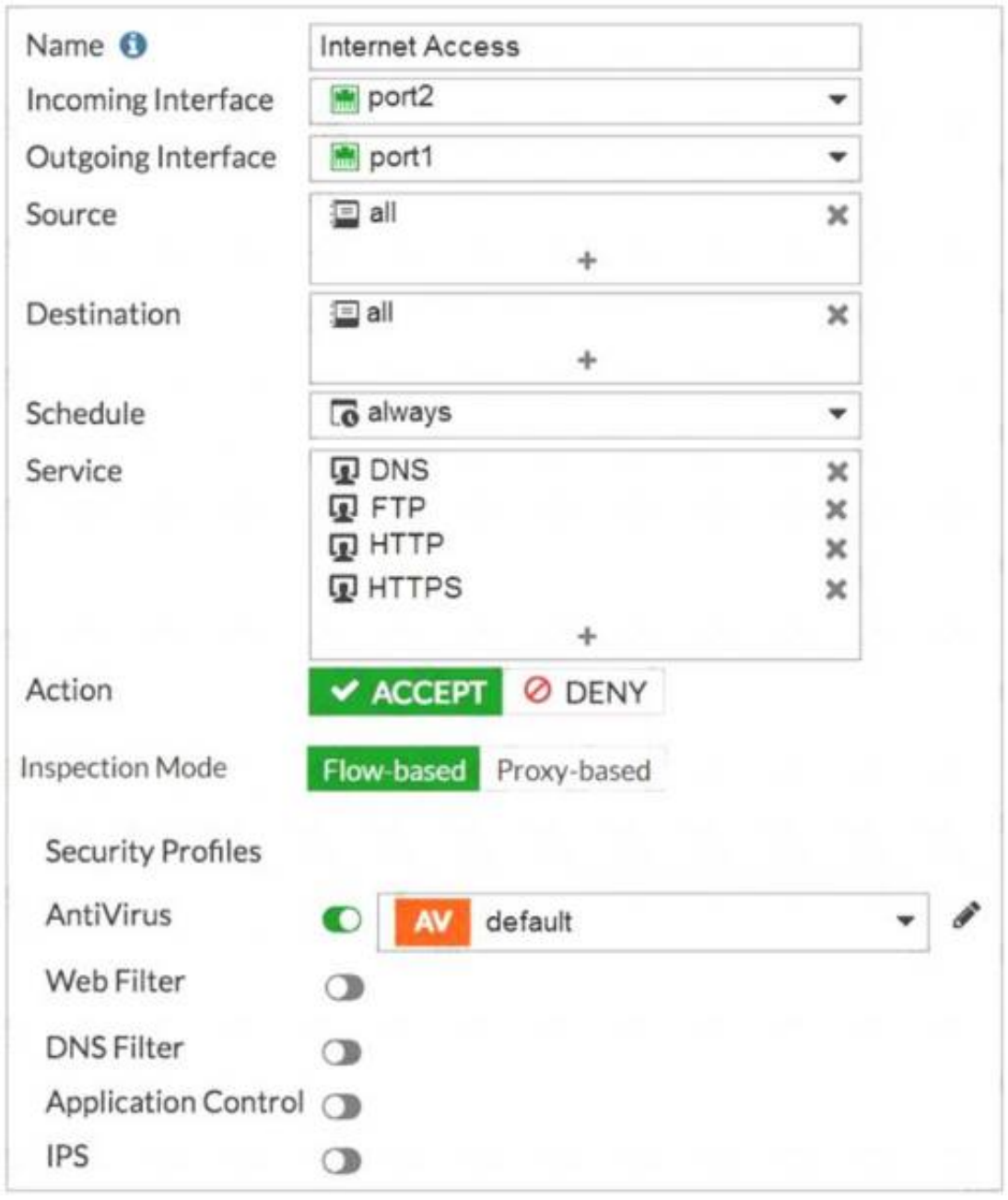
NEW QUESTION 60
- (Exam Topic 2)
The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.
What order must FortiGate use when the web filter profile has features enabled, such as safe search?

A. DNS-based web filter and proxy-based web filter
B. Static URL filter, FortiGuard category filter, and advanced filters
C. Static domain filter, SSL inspection filter, and external connectors filters
D. FortiGuard category filter and rating filter

Answer: B

Explanation:
Reference: https://fortinet121.rssing.com/chan-67705148/all_p1.html

NEW QUESTION 62
- (Exam Topic 2)
Refer to the exhibit to view the firewall policy.



Which statement is correct if well-known viruses are not being blocked?

A. The firewall policy does not apply deep content inspection.
B. The firewall policy must be configured in proxy-based inspection mode.
C. The action on the firewall policy must be set to deny.
D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

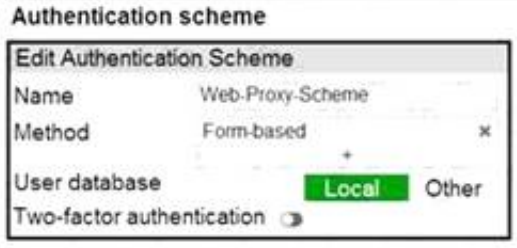
Answer: A

NEW QUESTION 67
- (Exam Topic 2)
Refer to the exhibit.

Authentication rule

Users

Authentication scheme

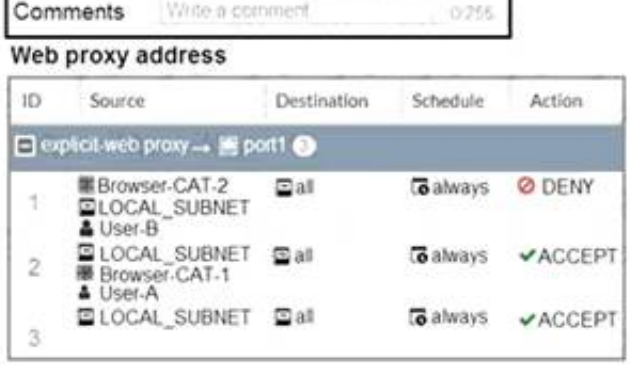


Firewall address

Proxy address

Proxy address

Web proxy address



The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.
An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies. The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a
form-based authentication scheme for the FortiGate local user database. Users will be prompted for
authentication.
How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP 10.1.1.10 to the destination http://www.fortinet.com? (Choose two.)

A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

Answer: BD

NEW QUESTION 71
- (Exam Topic 2)
View the exhibit.

Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.
B. Dead peer detection must be disabled to support this type of IPsec setup.
C. The TunnelB route is the primary route for reaching the remote sit
D. The TunnelA route is used only if the TunnelB VPN is down.
E. This is a redundant IPsec setup.

Answer: CD

NEW QUESTION 76
- (Exam Topic 2)
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

A. diagnose sys top
B. execute ping
C. execute traceroute
D. diagnose sniffer packet any
E. get system arp

Answer: BCD

NEW QUESTION 80
- (Exam Topic 2)
Exhibit:

```
Fortigate # show authentication rule
config authentication rule
    edit "NTLM_rule"
        set srcaddr "all"
        set ip-based disable
        set web-auth-cookie enable
    next
end
```

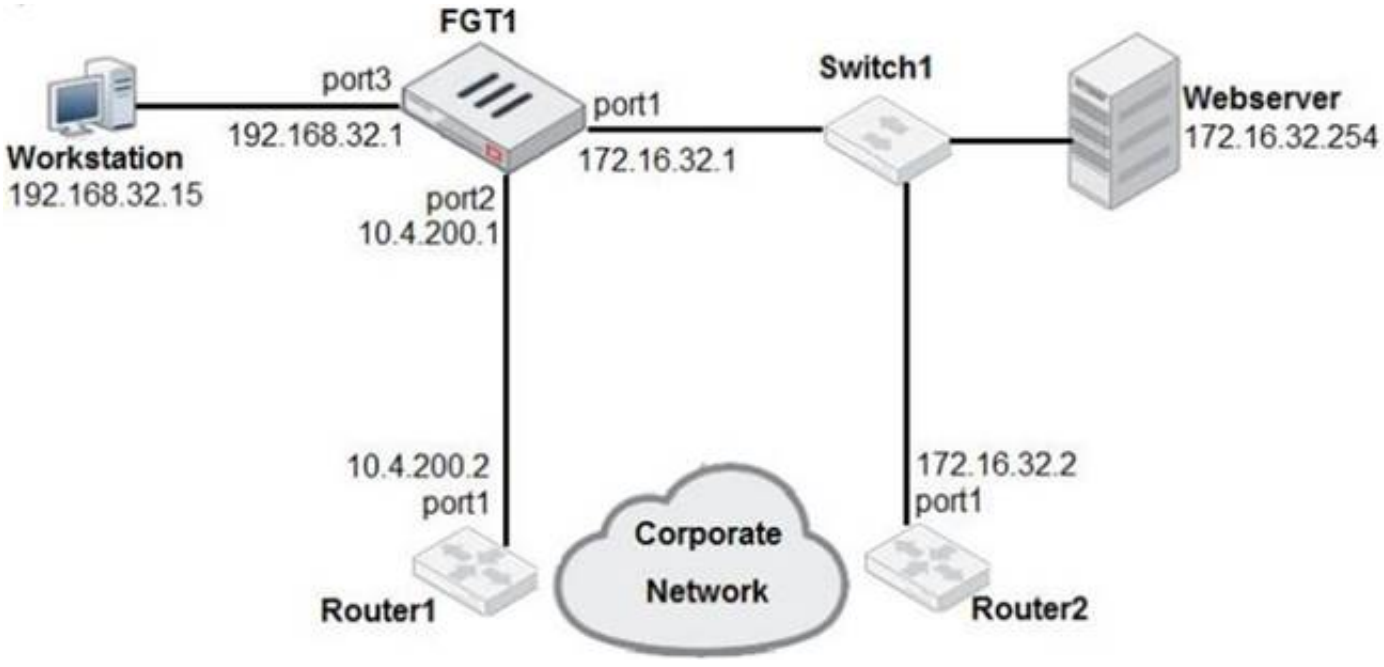
Refer to the exhibit to view the authentication rule configuration In this scenario, which statement is true?

A. IP-based authentication is enabled
B. Route-based authentication is enabled
C. Session-based authentication is enabled.
D. Policy-based authentication is enabled

Answer: C

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD45387

NEW QUESTION 83
- (Exam Topic 2)
Examine the network diagram shown in the exhibit, then answer the following question:



Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

A. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
B. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
C. 10.4.200.0/30 is directly connected, port2
D. 172.16.32.0/24 is directly connected, port1

Answer: D

NEW QUESTION 86
- (Exam Topic 2)
Which of the following statements about central NAT are true? (Choose two.)

A. IP tool references must be removed from existing firewall policies before enabling central NAT.
B. Central NAT can be enabled or disabled from the CLI only.
C. Source NAT, using central NAT, requires at least one central SNAT policy.
D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 87
- (Exam Topic 2)
Which of the following SD-WAN load –balancing method use interface weight value to distribute traffic? (Choose two.)

A. Source IP
B. Spillover
C. Volume
D. Session

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing

NEW QUESTION 92
- (Exam Topic 2)
An organization’s employee needs to connect to the office through a high-latency internet connection. Which SSL VPN setting should the administrator adjust to prevent the SSL VPN negotiation failure?

A. Change the session-ttl.
B. Change the login timeout.
C. Change the idle-timeout.
D. Change the udp idle timer.

Answer: B

NEW QUESTION 97
- (Exam Topic 2)
Refer to the exhibit.

Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?

A. Custom permission for Network
B. Read/Write permission for Log & Report
C. CLI diagnostics commands permission
D. Read/Write permission for Firewall

Answer: C

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220

NEW QUESTION 101
- (Exam Topic 2)
Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection
B. Antivirus in flow-based inspection
C. DNS filter
D. Web application firewall
E. Application control

Answer: ABE

NEW QUESTION 103
- (Exam Topic 2)
Which three methods are used by the collector agent for AD polling? (Choose three.)

A. FortiGate polling
B. NetAPI
C. Novell API
D. WMI
E. WinSecLog

Answer: BDE

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

NEW QUESTION 104
- (Exam Topic 2)

Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.
C. Highest to lowest priority defined in the firewall policy.
D. Services defined in the firewall policy.
E. Lowest to highest policy ID number.

Answer: ABD

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435

NEW QUESTION 109
- (Exam Topic 2)
If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

A. The Services field prevents SNAT and DNAT from being combined in the same policy.
B. The Services field is used when you need to bundle several VIPs into VIP groups.
C. The Services field removes the requirement to create multiple VIPs for different services.
D. The Services field prevents multiple sources of traffic from using multiple services to connect to a singlecomputer.

Answer: C

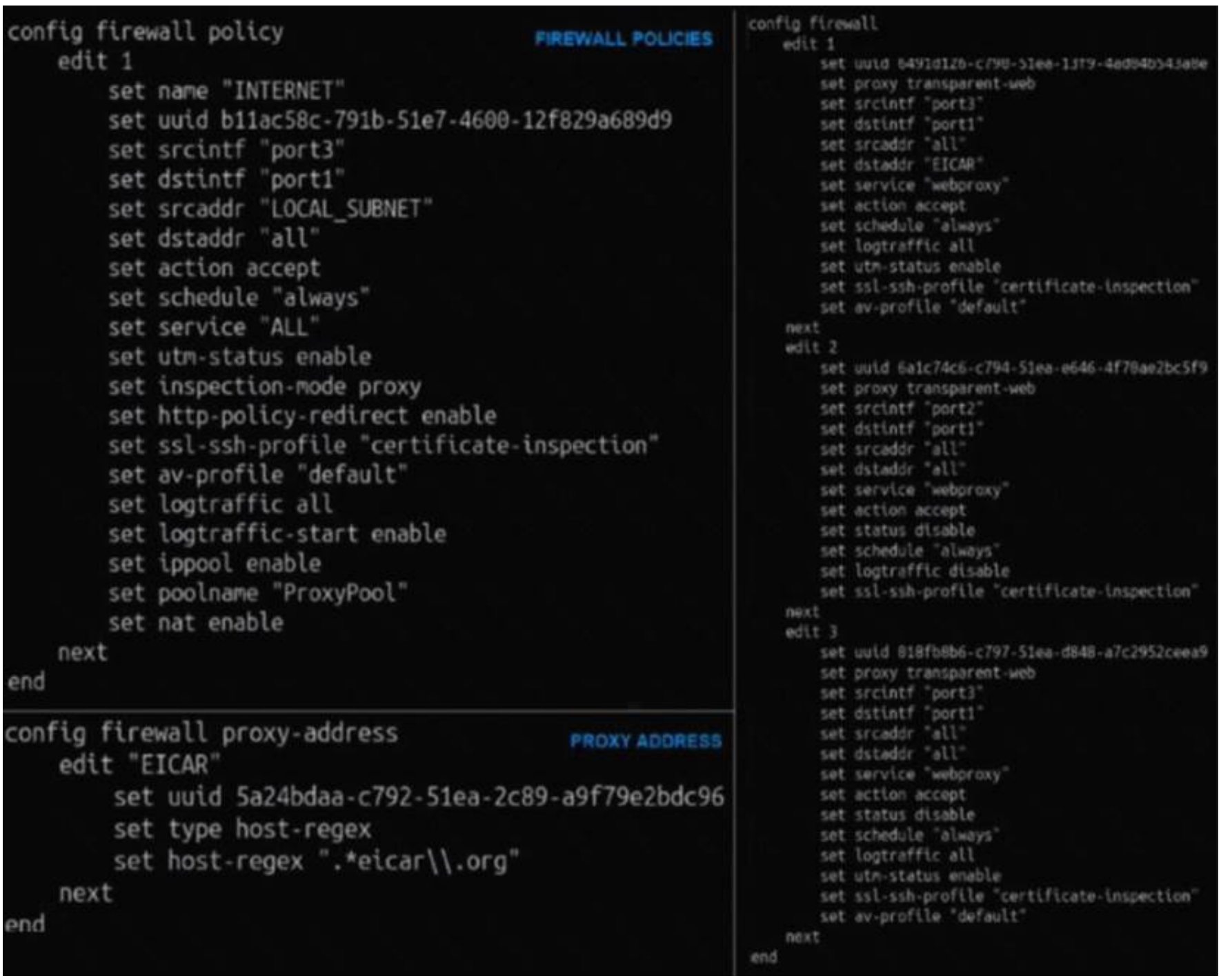
NEW QUESTION 112
- (Exam Topic 2)
An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface
B. Software Switch interface
C. Aggregate interface
D. Redundant interface

Answer: C

Explanation:
Reference: https://forum.fortinet.com/tm.aspx?m=120324

NEW QUESTION 116
- (Exam Topic 2)
Refer to the exhibit.



The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.
How does FortiGate process the traffic sent to http://www.fortinet.com?

A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
C. Traffic will be redirected to the transparent proxy and It will be allowed by proxy policy ID 1.
D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Answer: D

NEW QUESTION 120
- (Exam Topic 2)
Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

A. Root VDOM
B. FG-traffic VDOM
C. Customer VDOM
D. Global VDOM

Answer: A

NEW QUESTION 125
- (Exam Topic 2)
Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

A. Denial of Service
B. Web application firewall
C. Antivirus
D. Application control

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortiweb/6.3.3/administration-guide/60895/introduction

NEW QUESTION 126
- (Exam Topic 2)
Which two statements are true about collector agent advanced mode? (Choose two.)

A. Advanced mode uses Windows convention—NetBios: Domain\Username.
B. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate
C. Advanced mode supports nested or inherited groups
D. Security profiles can be applied only to user groups, not individual users.

Answer: BC

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso

NEW QUESTION 131
- (Exam Topic 2)
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view
B. Log backups from the CLI cannot be restored to another FortiGate.
C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

NEW QUESTION 133
- (Exam Topic 2)
An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.
B. This VPN cannot be used as part of a hub-and-spoke topology.
C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
D. The IPsec firewall policies must be placed at the top of the list.

Answer: C

Explanation:
In a route-based configuration, FortiGate automatically adds a virtual interface eith the VPN name (Infrastructure Study Guide, 206)

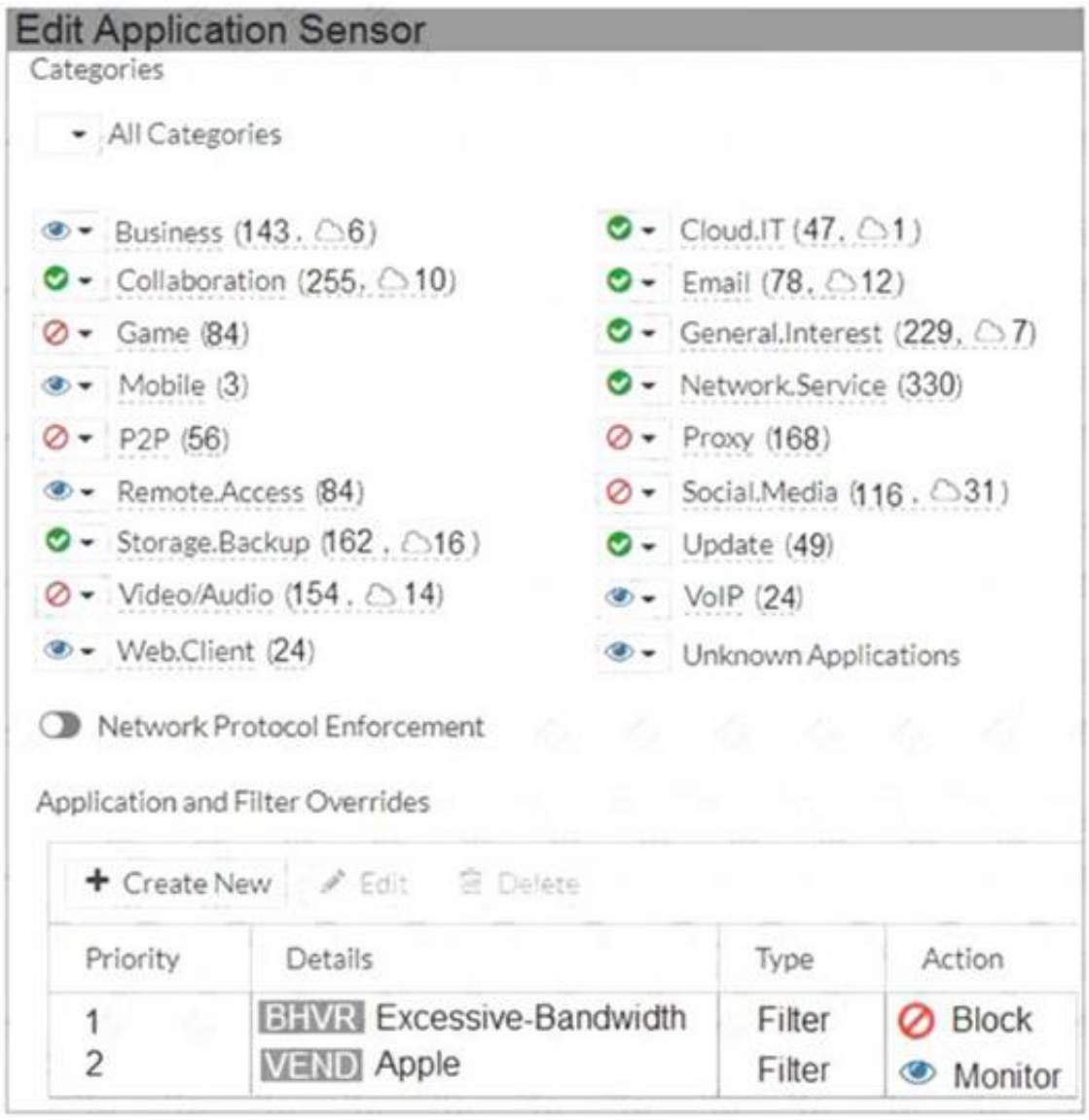
NEW QUESTION 135
- (Exam Topic 2)
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

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

Answer: ADE

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

NEW QUESTION 139
- (Exam Topic 2)
Refer to the exhibit to view the application control profile.



Users who use Apple FaceTime video conferences are unable to set up meetings. In this scenario, which statement is true?

A. Apple FaceTime belongs to the custom monitored filter.
B. The category of Apple FaceTime is being monitored.
C. Apple FaceTime belongs to the custom blocked filter.
D. The category of Apple FaceTime is being blocked.

Answer: C

NEW QUESTION 140
- (Exam Topic 2)
Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

A. Shut down/reboot a downstream FortiGate device.
B. Disable FortiAnalyzer logging for a downstream FortiGate device.
C. Log in to a downstream FortiSwitch device.
D. Ban or unban compromised hosts.

Answer: AB

NEW QUESTION 143
- (Exam Topic 2)
Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.
B. AH does not support perfect forward secrecy.
C. AH provides data integrity bur no encryption.
D. AH provides strong data integrity but weak encryption.

Answer: C

NEW QUESTION 148
- (Exam Topic 2)
Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

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

Answer: D

NEW QUESTION 151
- (Exam Topic 2)
Examine the two static routes shown in the exhibit, then answer the following question.

+ Create New	Edit	Clone	Delete		
Destination	Gateway	Interface	Priority	Distance	
172.20.168.0/24	172.25.176.1	port1	10	20	
172.20.168.0/24	172.25.178.1	port2	20	20	

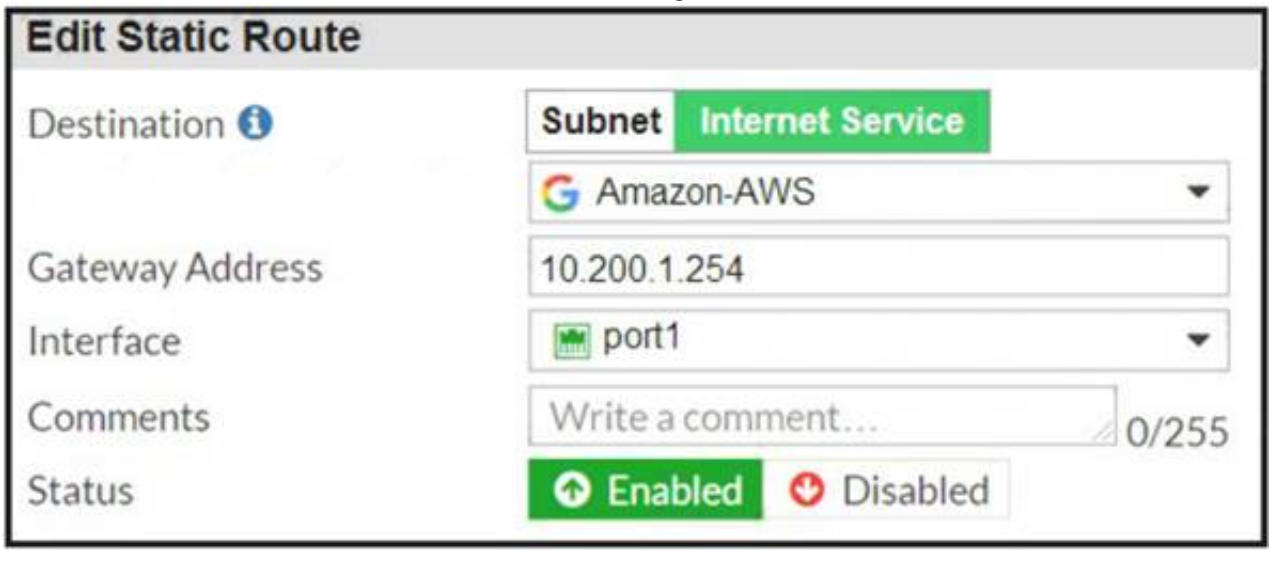
Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.
B. FortiGate will use the port1 route as the primary candidate.
C. FortiGate will route twice as much traffic to the port2 route
D. FortiGate will only actuate the port1 route in the routing table

Answer: B

Explanation:
"If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path."

NEW QUESTION 153
- (Exam Topic 2)
Refer to the exhibit, which contains a static route configuration.



An administrator created a static route for Amazon Web Services. What CLI command must the administrator use to view the route?

A. get router info routing-table all
B. get internet service route list
C. get router info routing-table database
D. diagnose firewall proute list

Answer: D

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/latest/administration-guide/139692/routing-concepts

NEW QUESTION 157
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

NSE4_FGT-7.0 Practice Exam Features:

* NSE4_FGT-7.0 Questions and Answers Updated Frequently

* NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year