[May 23, 2022 Fortinet NSE4_FGT-7.0 Real Exam Questions and Answers FREE [Q64-Q88

[May 23, 2022] Fortinet NSE4_FGT-7.0 Real Exam Questions and Answers FREE
Pass Fortinet NSE4_FGT-7.0 Exam Info and Free Practice Test

Fortinet NSE4_FGT-7.0 Exam Syllabus Topics:

TopicDetailsTopic 1- Explain and configure antivirus scanning modes to neutralize malware threats- Identify FortiGate inspection modes and configure web and DNS filteringTopic 2- Identify and configure different methods of firewall authentication- Describe and inspect encrypted traffic using certificatesTopic 3- Configure and implement different SSL-VPN modes to provide secure access to the private network- Implement the Fortinet Security FabricTopic 4- Implement a meshed or partially redundant IPsec VPN- Explain FSSO deployment and configuration

NO.64 Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

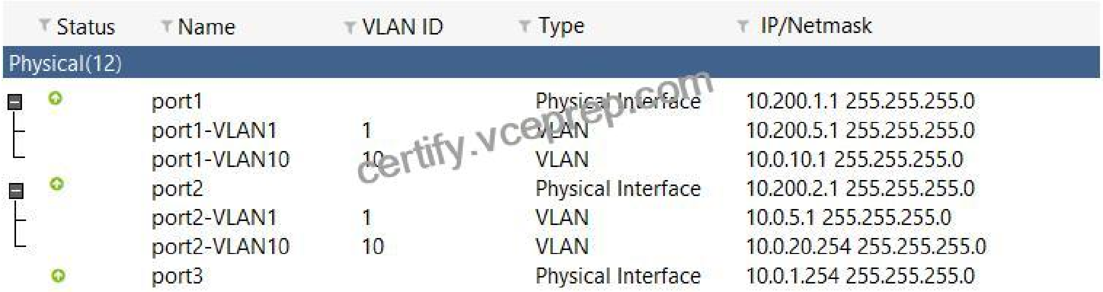
* The public key of the web server certificate must be installed on the browser.
* The web-server certificate must be installed on the browser.
* The CA certificate that signed the web-server certificate must be installed on the browser.

* The private key of the CA certificate that signed the browser certificate must be installed on the browser.

NO.65 Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)
* FortiGate points the collector agent to use a remote LDAP server.
* FortiGate uses the AD server as the collector agent.
* FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
* FortiGate queries AD by using the LDAP to retrieve user group information.
Fortigate Infrastructure 7.0 Study Guide P.272-273

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

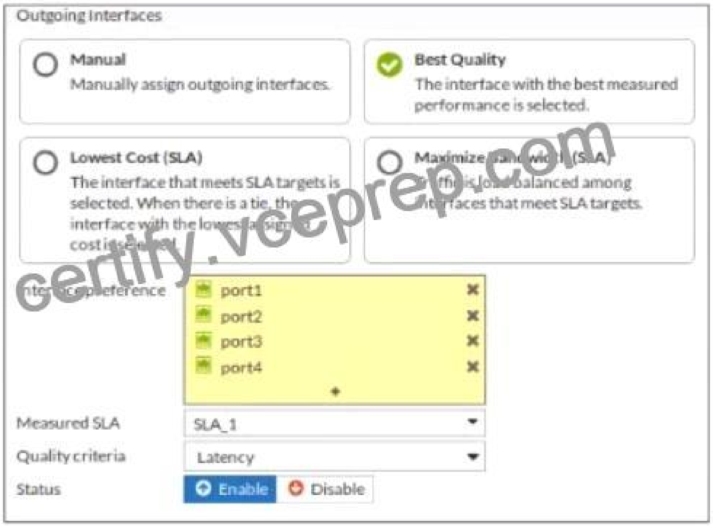
NO.66 View the exhibit:



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.)
* Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
* port-VLAN1 is the native VLAN for the port1 physical interface.
* port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
* Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

NO.67 Refer to the exhibit.



Outgoing Interfaces

○ Manual
Manually assign outgoing interfaces.

● Best Quality
The interface with the best measured performance is selected.

○ Lowest Cost (SLA)
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

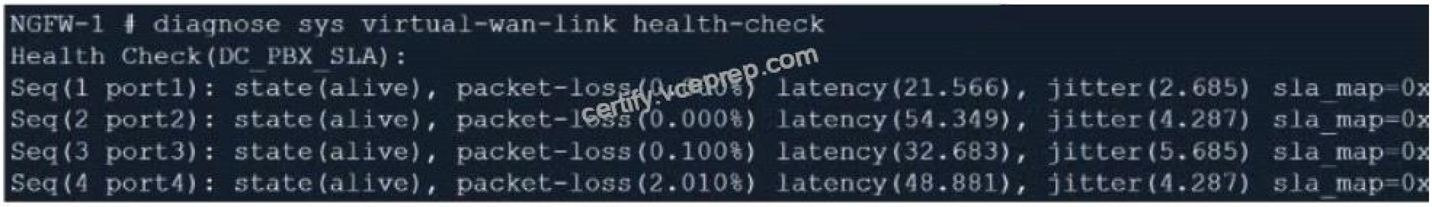
○ Maximize Bandwidth (SLA)
Traffic is load balanced among interfaces that meet SLA targets.

Interface preference: port1, port2, port3, port4

Measured SLA: SLA_1

Quality criteria: Latency

Status: Enable [✓] Disable

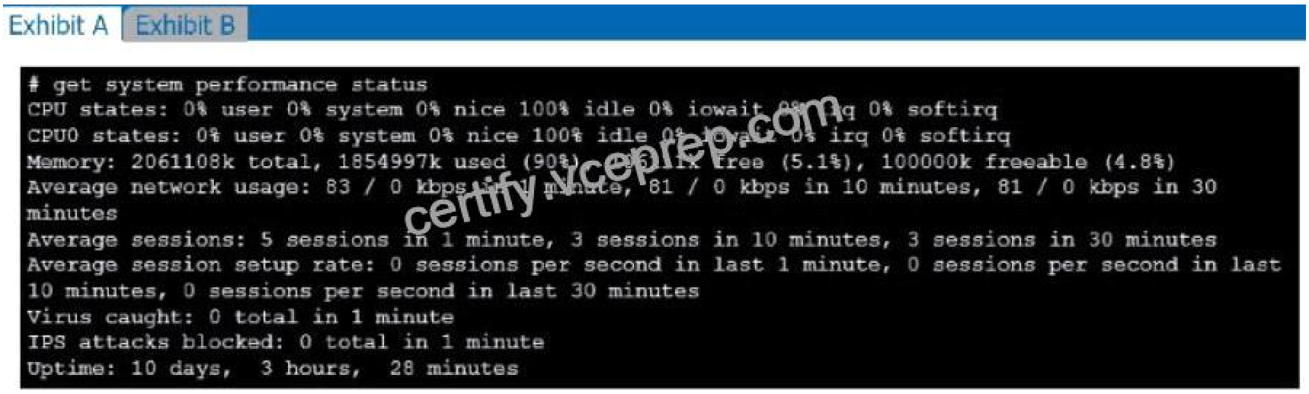


```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

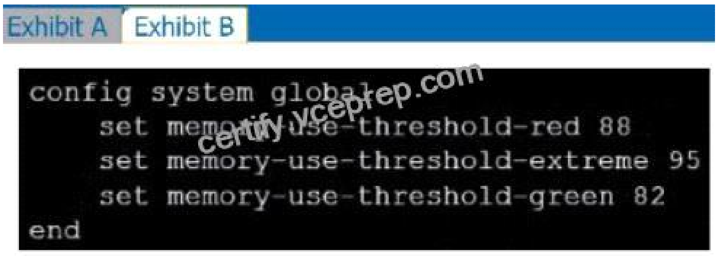
The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check.

Which interface will be selected as an outgoing interface?
* port2
* port4
* port3
* port1
Port 1 shows the lowest latency.

NO.68 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%), 206111k 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.)
* Administrators can access FortiGate only through the console port.
* FortiGate has entered conserve mode.
* FortiGate will start sending all files to FortiSandbox for inspection.
* Administrators cannot change the configuration.

NO.69 Which statement about video filtering on FortiGate is true?
* Full SSL Inspection is not required.
* It is available only on a proxy-based firewall policy.
* It inspects video files hosted on file sharing services.
* Video filtering FortiGuard categories are based on web filter FortiGuard categories.

NO.70 An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)
* The interface has been configured for one-arm sniffer.
* The interface is a member of a virtual wire pair.
* The operation mode is transparent.
* The interface is a member of a zone.
* Captive portal is enabled in the interface.
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

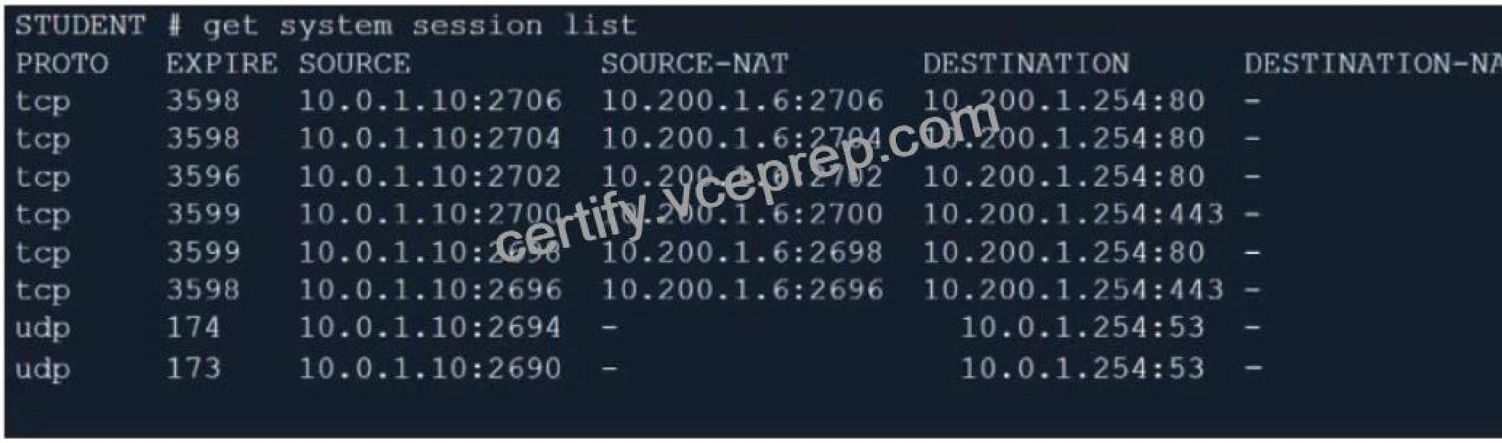
NO.71 What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?
* It limits the scanning of application traffic to the DNS protocol only.
* It limits the scanning of application traffic to use parent signatures only.
* It limits the scanning of application traffic to the browser-based technology category only.
* It limits the scanning of application traffic to the application category only.

NO.72 An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.12" 5
```

Which three pieces of Information will be Included in me sniffer output? {Choose three.)
* Interface name
* Packet payload
* Ethernet header
* IP header
* Application header

NO.73 Refer to the exhibit.



```
STUDENT # get system session list
PROTO   EXPIRE SOURCE            SOURCE-NAT         DESTINATION          DESTINATION-NA
tcp     3598   10.0.1.10:2706    10.200.1.6:2706    10.200.1.254:80      -
tcp     3598   10.0.1.10:2704    10.200.1.6:2704    10.200.1.254:80      -
tcp     3596   10.0.1.10:2702    10.200.1.6:2702    10.200.1.254:80      -
tcp     3599   10.0.1.10:2700    10.200.1.6:2700    10.200.1.254:443     -
tcp     3599   10.0.1.10:2698    10.200.1.6:2698    10.200.1.254:80      -
tcp     3598   10.0.1.10:2696    10.200.1.6:2696    10.200.1.254:443     -
udp     174    10.0.1.10:2694    -                    10.0.1.254:53      -
udp     173    10.0.1.10:2690    -                    10.0.1.254:53      -
```

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?
* Destination NAT is disabled in the firewall policy.
* One-to-one NAT IP pool is used in the firewall policy.
* Overload NAT IP pool is used in the firewall policy.
* Port block allocation IP pool is used in the firewall policy.

FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

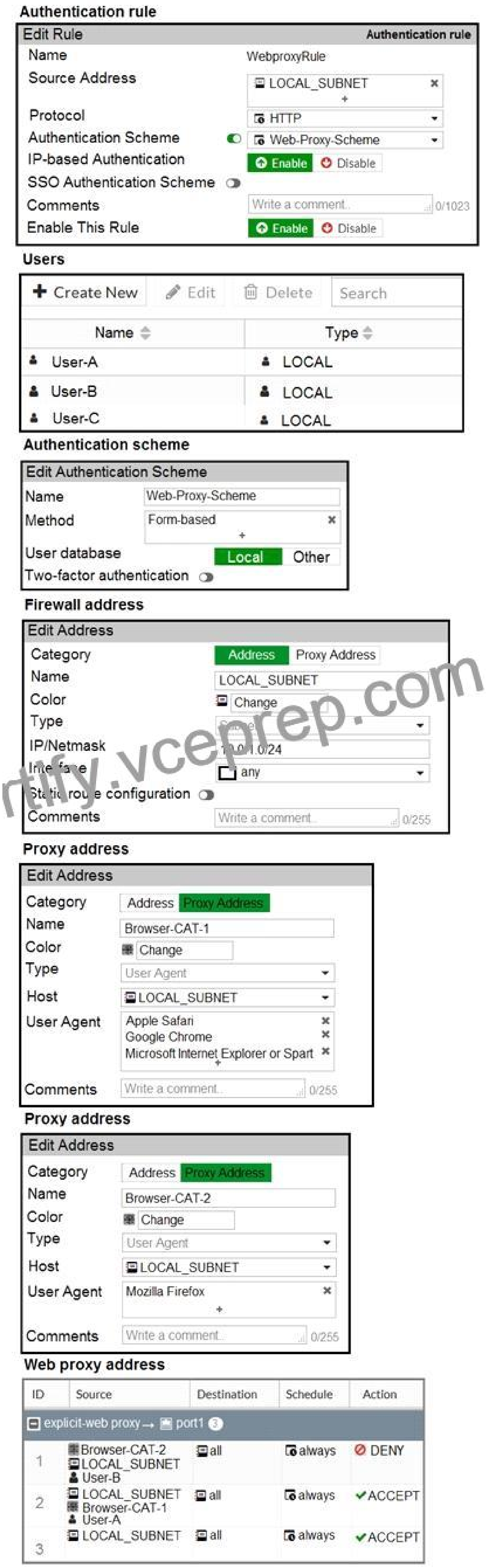
NO.74 Which statements best describe auto discovery VPN (ADVPN). (Choose two.)
* It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
* ADVPN is only supported with IKEv2.
* Tunnels are negotiated dynamically between spokes.
* Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

NO.75 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?
* Add the support of NTLM authentication.
* Add user accounts to Active Directory (AD).
* Add user accounts to the FortiGate group fitter.
* Add user accounts to the Ignore User List.

NO.76 In an explicit proxy setup, where is the authentication method and database configured?
* Proxy Policy
* Authentication Rule
* Firewall Policy
* Authentication scheme

NO.77 Which three statements about a flow-based antivirus profile are correct? (Choose three.)
* IPS engine handles the process as a standalone.
* FortiGate buffers the whole file but transmits to the client simultaneously.
* If the virus is detected, the last packet is delivered to the client.
* Optimized performance compared to proxy-based inspection.
* Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

NO.78 Refer to the exhibit.



Authentication rule

Edit Rule — Authentication rule

Name	WebproxyRule
Source Address	LOCAL_SUBNET
Protocol	HTTP
Authentication Scheme	Web-Proxy-Scheme
IP-based Authentication	[✓ Enable] Disable
SSO Authentication Scheme	
Comments	Write a comment. 0/1023
Enable This Rule	[✓ Enable] Disable

Users

Create New | Edit | Delete | Search

Name	Type
User-A	LOCAL
User-B	LOCAL
User-C	LOCAL

Authentication scheme

Edit Authentication Scheme

Name	Web-Proxy-Scheme
Method	Form-based
User database	[✓ Local] Other
Two-factor authentication	

Firewall address

Edit Address

Category	[✓ Address] Proxy Address
Name	LOCAL_SUBNET
Color	Change
Type	Subnet
IP/Netmask	10.0.1.0/24
Interface	any
Static route configuration	
Comments	Write a comment. 0/255

Proxy address

Edit Address

Category	Address [✓ Proxy Address]
Name	Browser-CAT-1
Color	Change
Type	User Agent
Host	LOCAL_SUBNET
User Agent	Apple Safari Google Chrome Microsoft Internet Explorer or Spart
Comments	Write a comment. 0/255

Proxy address

Edit Address

Category	Address [✓ Proxy Address]
Name	Browser-CAT-2
Color	Change
Type	User Agent
Host	LOCAL_SUBNET
User Agent	Mozilla Firefox
Comments	Write a comment. 0/255

Web proxy address

explicit-web proxy → port1 3

ID	Source	Destination	Schedule	Action
1	Browser-CAT-2 LOCAL_SUBNET User-B	all	always	DENY
2	LOCAL_SUBNET Browser-CAT-1 User-A	all	always	✓ACCEPT
3	LOCAL_SUBNET	all	always	✓ACCEPT

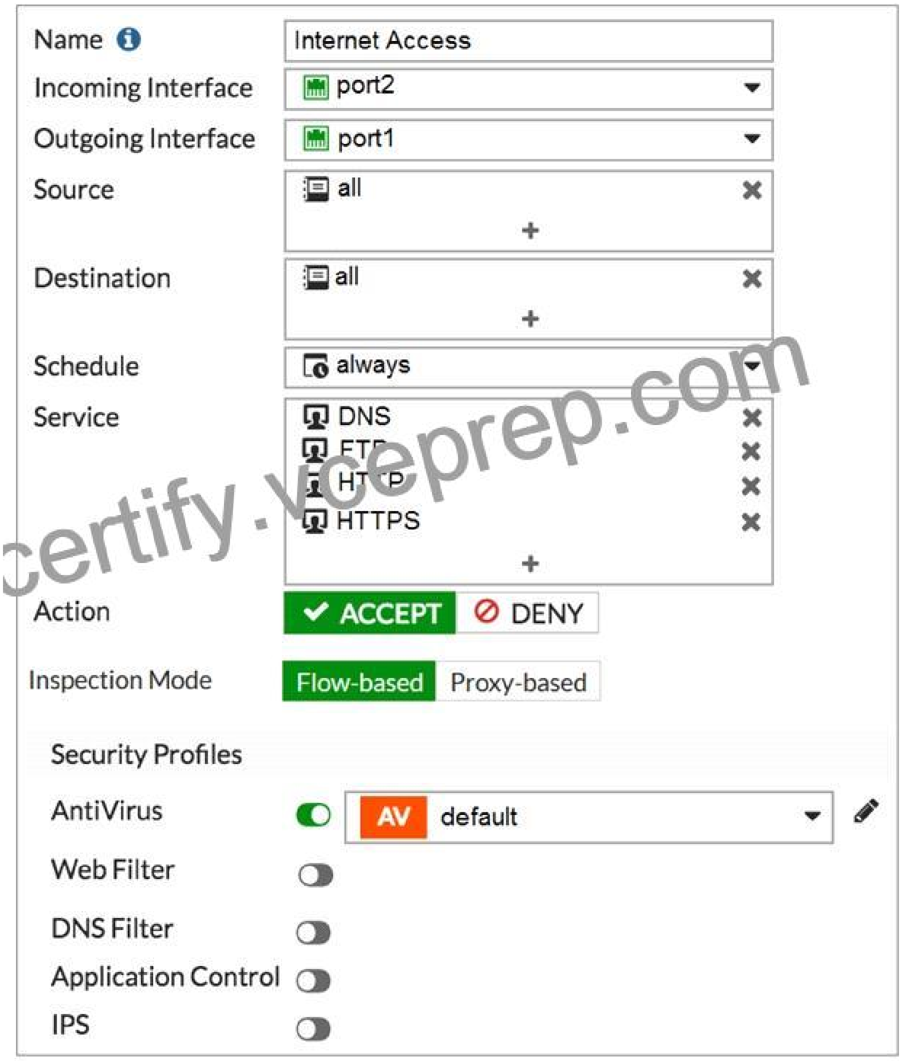
The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address.

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 10.0.1.10 to the destination http://www.fortinet.com? (Choose two.)
* If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
* If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
* If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
* If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

NO.79 Refer to the exhibit to view the firewall policy.



Name	Internet Access
Incoming Interface	port2
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	DNS FTP HTTP HTTPS
Action	[✓ ACCEPT] DENY
Inspection Mode	[✓ Flow-based] Proxy-based

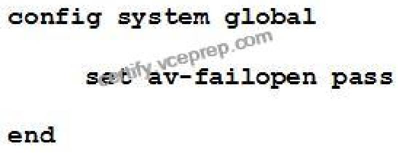
Security Profiles

AntiVirus	● AV default
Web Filter	○
DNS Filter	○
Application Control	○
IPS	○

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

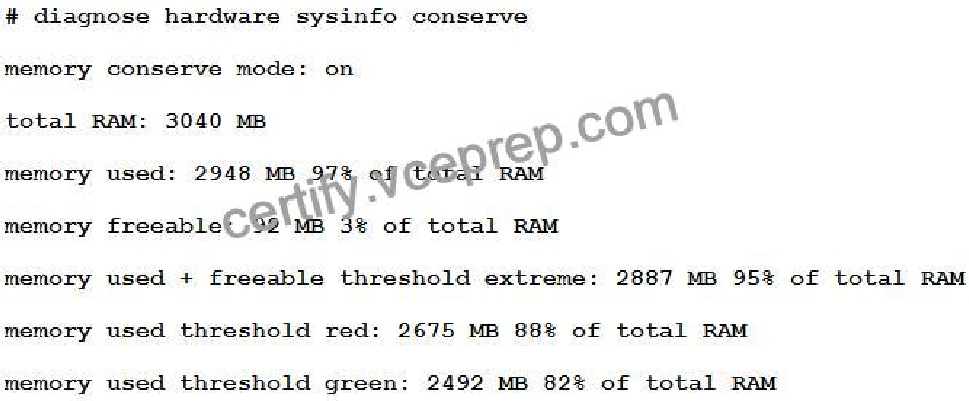
- The firewall policy does not apply deep content inspection.
- The firewall policy must be configured in proxy-based inspection mode.
- The action on the firewall policy must be set to deny.
- Web filter should be enabled on the firewall policy to complement the antivirus profile.

NO.80 Examine this FortiGate configuration:



```
config system global
     set av-failopen pass
end
```

Examine the output of the following debug command:



```
# diagnose hardware sysinfo conserve
memory conserve mode: on
total RAM: 3040 MB
memory used: 2948 MB 97% of total RAM
memory freeable: 92 MB 3% of total RAM
memory used + freeable threshold extreme: 2887 MB 95% of total RAM
memory used threshold red: 2675 MB 88% of total RAM
memory used threshold green: 2492 MB 82% of total RAM
```

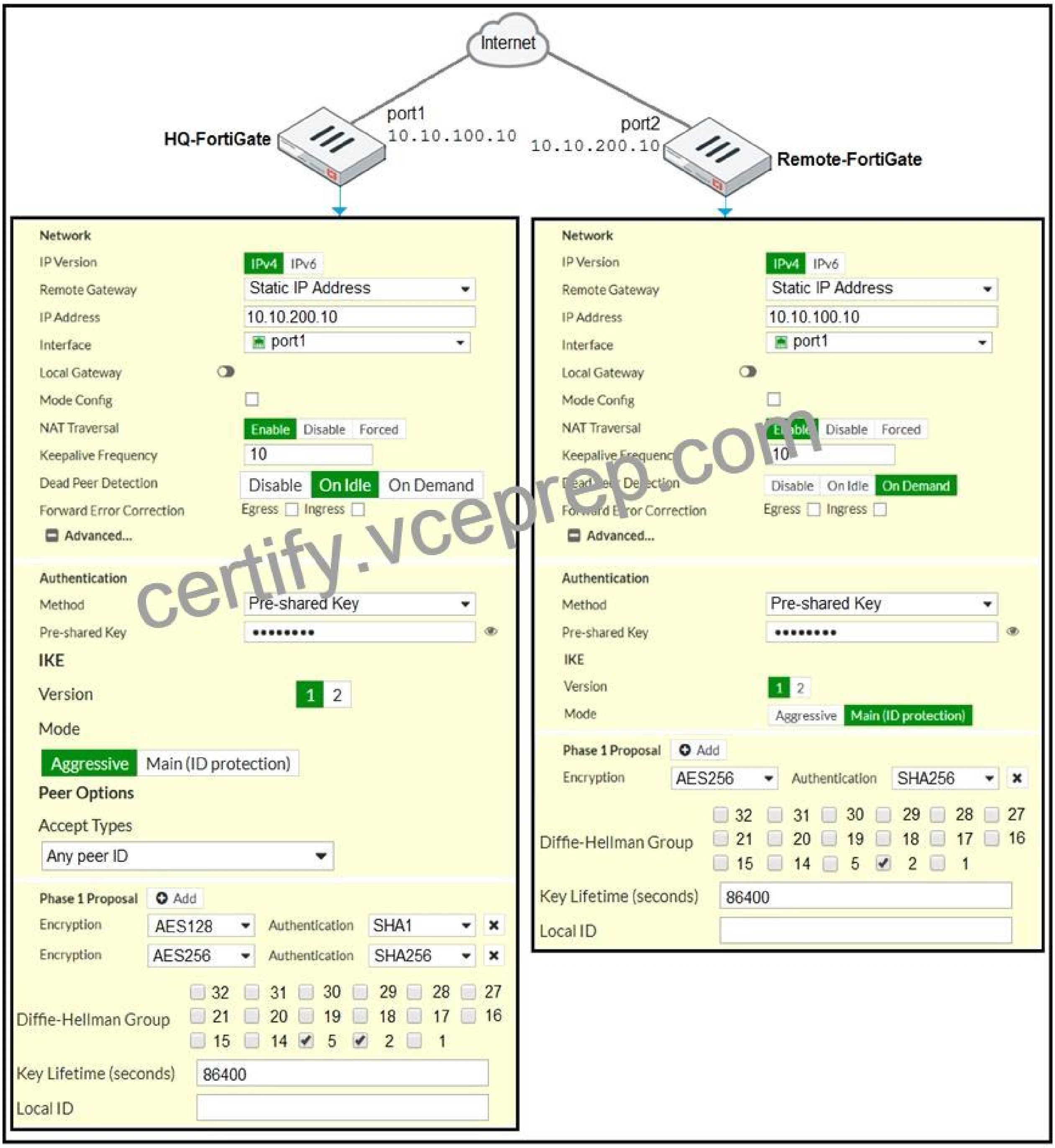
Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

- It is allowed, but with no inspection
- It is allowed and inspected as long as the inspection is flow based
- It is dropped.
- It is allowed and inspected, as long as the only inspection required is antivirus.

NO.81 Which of the following statements about central NAT are true? (Choose two.)

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

NO.82 Refer to the exhibit.



HQ-FortiGate

Network
IP Version [✓ IPv4] IPv6
Remote Gateway: Static IP Address
IP Address: 10.10.200.10
Interface: port1
Local Gateway
Mode Config □
NAT Traversal [✓ Enable] Disable Forced
Keepalive Frequency: 10
Dead Peer Detection: Disable [✓ On Idle] On Demand
Forward Error Correction: Egress □ Ingress □
Advanced...

Authentication
Method: Pre-shared Key
Pre-shared Key: ••••••••
IKE
Version [✓ 1] 2
Mode
[✓ Aggressive] Main (ID protection)
Peer Options
Accept Types: Any peer ID

Phase 1 Proposal Add
Encryption: AES128 Authentication: SHA1
Encryption: AES256 Authentication: SHA256
Diffie-Hellman Group
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 □ 14 ☑ 5 ☑ 2 □ 1
Key Lifetime (seconds): 86400
Local ID:

Remote-FortiGate

Network
IP Version [✓ IPv4] IPv6
Remote Gateway: Static IP Address
IP Address: 10.10.100.10
Interface: port1
Local Gateway
Mode Config □
NAT Traversal [✓ Enable] Disable Forced
Keepalive Frequency: 10
Dead Peer Detection: Disable On Idle [✓ On Demand]
Forward Error Correction: Egress □ Ingress □
Advanced...

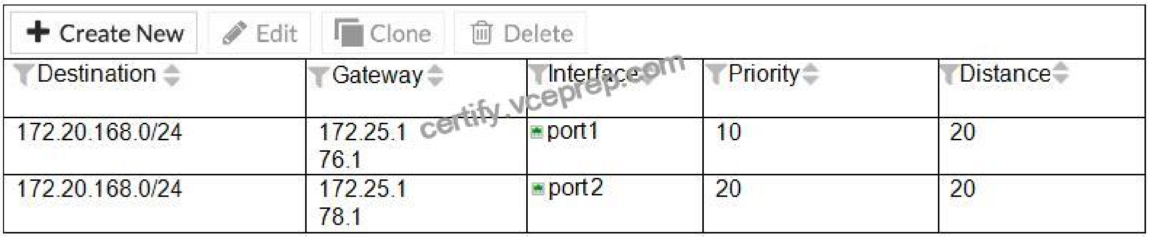
Authentication
Method: Pre-shared Key
Pre-shared Key: ••••••••
IKE
Version [✓ 1] 2
Mode: Aggressive [✓ Main (ID protection)]

Phase 1 Proposal Add
Encryption: AES256 Authentication: SHA256
Diffie-Hellman Group
□ 32 □ 31 □ 30 □ 29 □ 28 □ 27
□ 21 □ 20 □ 19 □ 18 □ 17 □ 16
□ 15 □ 14 □ 5 ☑ 2 □ 1
Key Lifetime (seconds): 86400
Local ID:

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

NO.83 Examine the two static routes shown in the exhibit, then answer the following question.

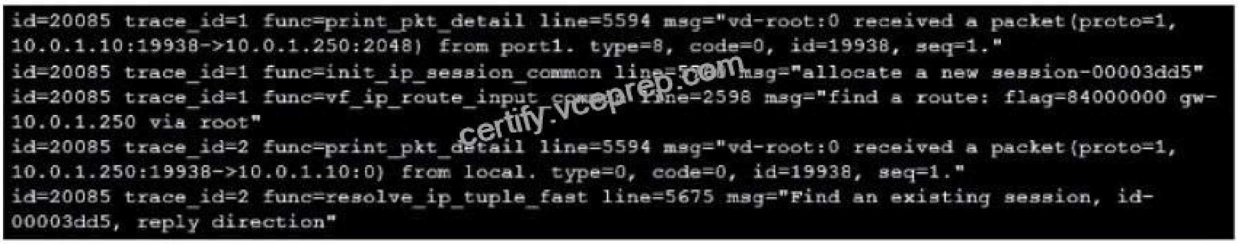


Destination	Gateway	Interface	Priority	Distance
172.20.168.0/24	172.25.176.1	port1	10	20
172.20.168.0/24	172.25.178.1	port2	20	20

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?
* FortiGate will load balance all traffic across both routes.
* FortiGate will use the port1 route as the primary candidate.
* FortiGate will route twice as much traffic to the port2 route
* FortiGate will only actuate the port1 route in the routing table

&#8220;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.&#8221;

NO.84 Refer to the exhibit showing a debug flow output.



```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=[illegible] msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw-
10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1,
10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)
* The debug flow is of ICMP traffic.
* A firewall policy allowed the connection.
* A new traffic session is created.
* The default route is required to receive a reply.

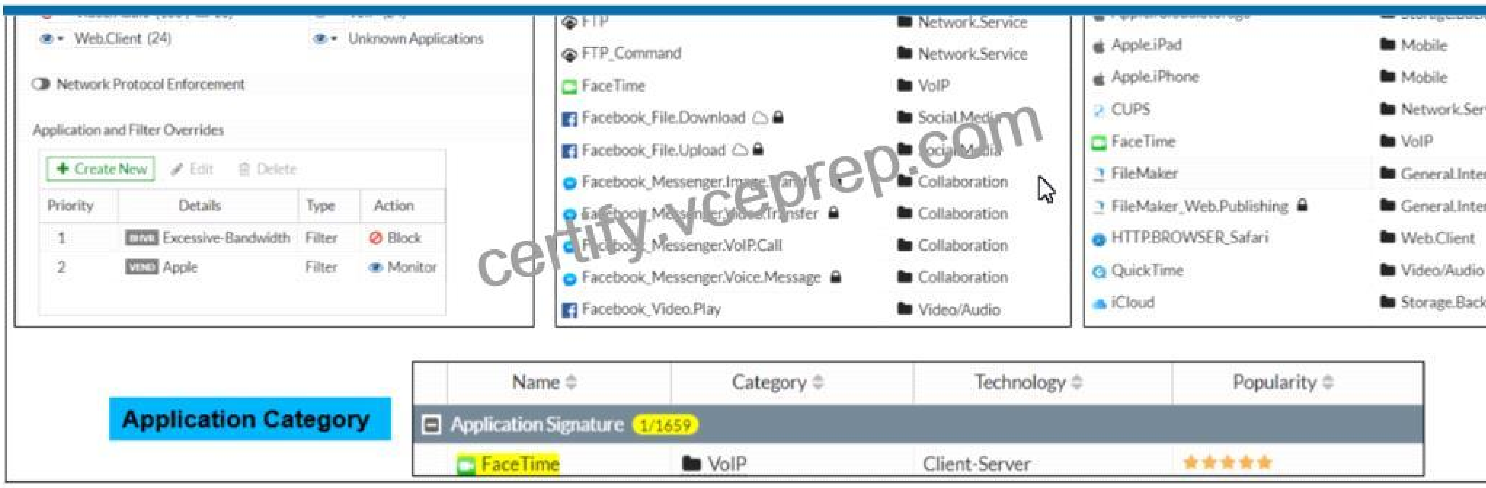
NO.85 Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)
* hard-timeout
* auth-on-demand
* soft-timeout
* new-session
* Idle-timeout

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

NO.86 Which two statements are true about the FGCP protocol? (Choose two.)
* Not used when FortiGate is in Transparent mode
* Elects the primary FortiGate device

- Runs only over the heartbeat links
- Is used to discover FortiGate devices in different HA groups

NO.87 Refer to the exhibit to view the application control profile.



Web.Client (24)
Unknown Applications
Network Protocol Enforcement
Application and Filter Overrides
Create New
Edit
Delete

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	Block
2	Apple	Filter	Monitor

FTP	Network.Service
FTP_Command	Network.Service
FaceTime	VoIP
Facebook_File.Download	Social.Media
Facebook_File.Upload	Social.Media
Facebook_Messenger.Image.Transfer	Collaboration
Facebook_Messenger.Video.Transfer	Collaboration
Facebook_Messenger.VoIP.Call	Collaboration
Facebook_Messenger.Voice.Message	Collaboration
Facebook_Video.Play	Video/Audio

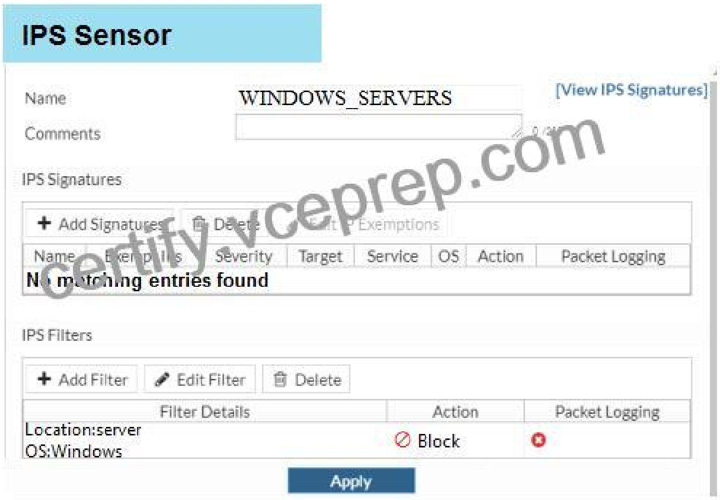
Apple.iPad	Mobile
Apple.iPhone	Mobile
CUPS	Network.Ser
FaceTime	VoIP
FileMaker	General.Inte
FileMaker_Web.Publishing	General.Inte
HTTP.BROWSER_Safari	Web.Client
QuickTime	Video/Audio
iCloud	Storage.Back

Name	Category	Technology	Popularity
Application Signature 1/1659			
FaceTime	VoIP	Client-Server	★★★★★

Based on the configuration, what will happen to Apple FaceTime?

- Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
- Apple FaceTime will be allowed, based on the Apple filter configuration.
- Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
- Apple FaceTime will be allowed, based on the Categories configuration.

NO.88 Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.



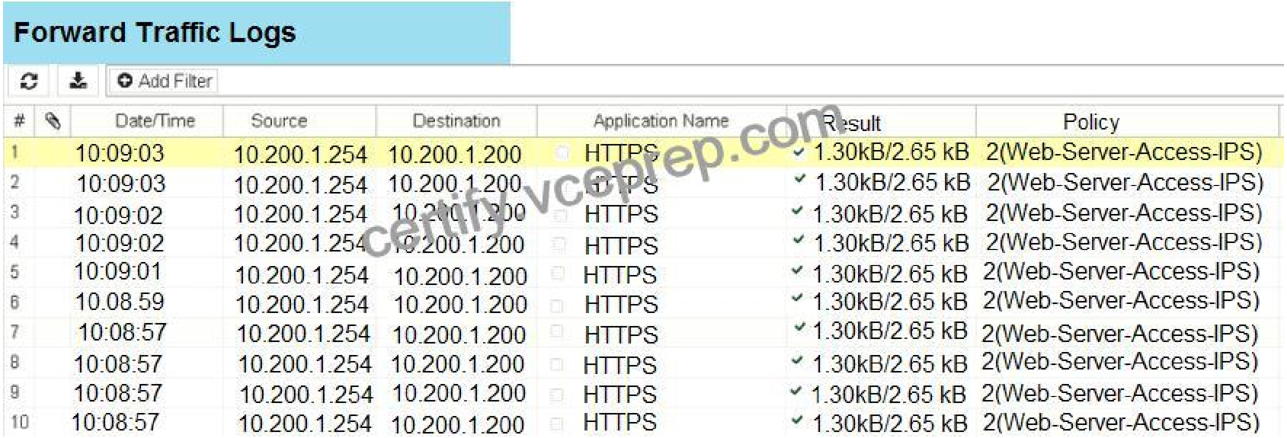
IPS Sensor

Name: WINDOWS_SERVERS

Comments:

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
No matching entries found							

Filter Details	Action	Packet Logging
Location:server OS:Windows	Block	✗



Forward Traffic Logs

#		Date/Time	Source	Destination	Application Name	Result	Policy
1		10:09:03	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
2		10:09:03	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
3		10:09:02	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
4		10:09:02	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
5		10:09:01	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
6		10.08.59	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
7		10:08:57	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
8		10:08:57	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
9		10:08:57	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)
10		10:08:57	10.200.1.254	10.200.1.200	□ HTTPS	✓ 1.30kB/2.65 kB	2(Web-Server-Access-IPS)

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.

What is a possible reason for this?
* The IPS filter is missing the Protocol: HTTPS option.
* The HTTPS signatures have not been added to the sensor.
* A DoS policy should be used, instead of an IPS sensor.
* A DoS policy should be used, instead of an IPS sensor.
* The firewall policy is not using a full SSL inspection profile.

Latest NSE4_FGT-7.0 Exam Dumps Fortinet Exam: https://www.vceprep.com/NSE4_FGT-7.0-latest-vce-prep.html]