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 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 3
- (Exam Topic 1)
Refer to the exhibit.

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. The signature setting uses a custom rating threshold.
B. The signature setting includes a group of other signatures.
C. Traffic matching the signature will be allowed and logged.
D. Traffic matching the signature will be silently dropped and logged.

Answer: D

Explanation:
Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

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 type of logs on FortiGate record information about traffic directly to and from the FortiGate management IP addresses?
A. System event logs
B. Forward traffic logs
C. Local traffic logs
D. Security logs

Answer: C

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970

NEW QUESTION 6
- (Exam Topic 1)
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

Answer: CD

NEW QUESTION 7
- (Exam Topic 1)
Which two statements about antivirus scanning mode are true? (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.

Answer: BC

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.

NEW QUESTION 8
- (Exam Topic 1)
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.

Answer: A

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
Refer to the exhibit.

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

Answer: C

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

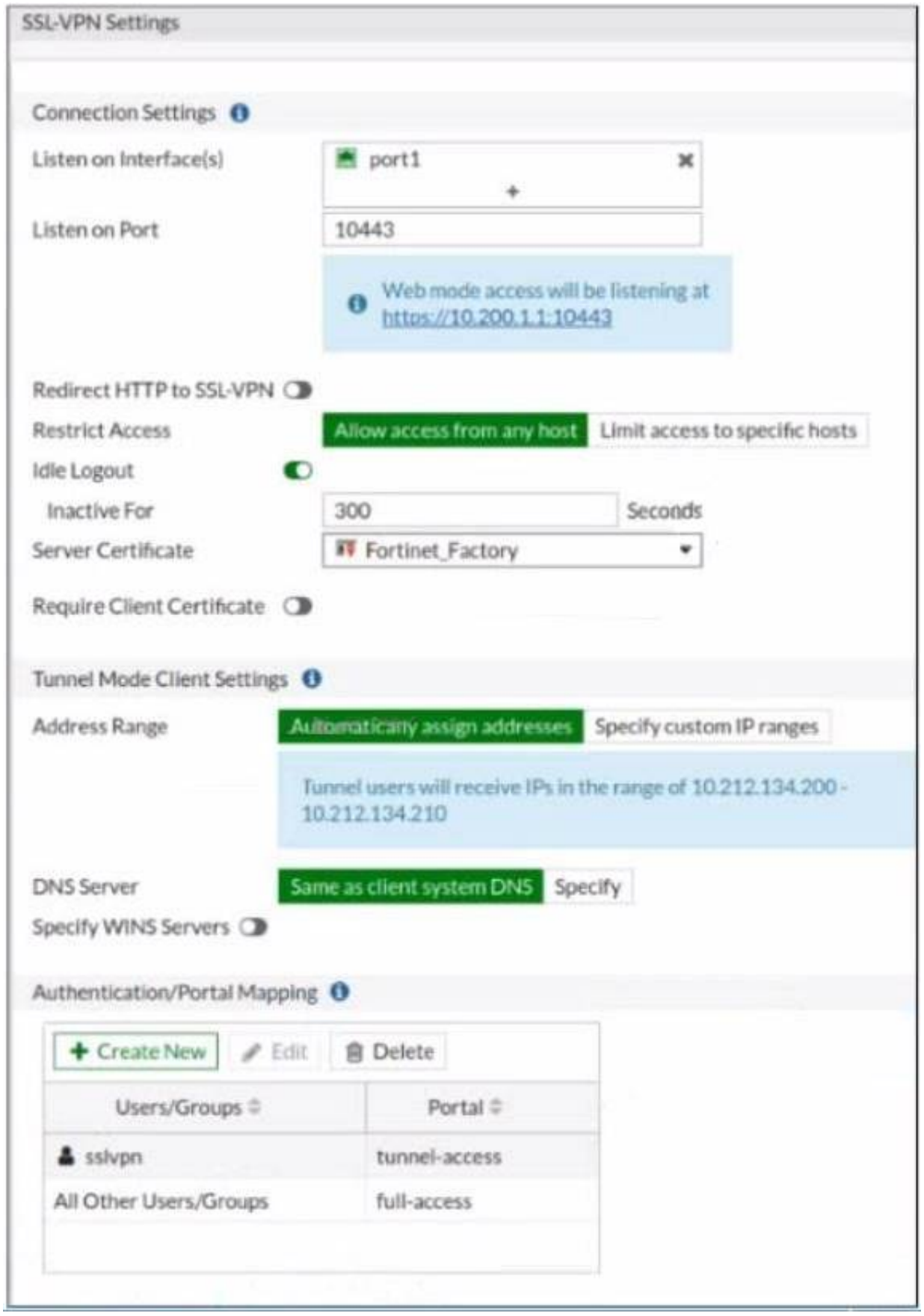
NEW QUESTION 10
- (Exam Topic 1)
Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

A. The keyUsage extension must be set to keyCertSign.
B. The common name on the subject field must use a wildcard name.
C. The issuer must be a public CA.
D. The CA extension must be set to TRUE.

Answer: AD

Explanation:
Reference: https://www.reddit.com/r/fortinet/comments/c7j6jg/recommended_ssl_cert/

NEW QUESTION 12
- (Exam Topic 1)
Refer to the exhibits.



The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

A. Change the SSL VPN port on the client.
B. Change the Server IP address.
C. Change the idle-timeout.
D. Change the SSL VPN portal to the tunnel.

Answer: A

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/150494

NEW QUESTION 16
- (Exam Topic 1)

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.168.1.0/24 and the remote quick mode selector is 192.168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192.168.1.0/24
B. 192.168.0.0/24
C. 192.168.2.0/24
D. 192.168.3.0/24

Answer: C

NEW QUESTION 18
- (Exam Topic 1)
Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

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

Answer: AB

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

NEW QUESTION 22
- (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 27
- (Exam Topic 1)
An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```

What are the two results of this configuration? (Choose two.)

A. Device detection on all interfaces is enforced for 30 minutes.
B. Denied users are blocked for 30 minutes.
C. A session for denied traffic is created.
D. The number of logs generated by denied traffic is reduced.

Answer: CD

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328

NEW QUESTION 31
- (Exam Topic 1)
Refer to the exhibits.
Exhibit A.

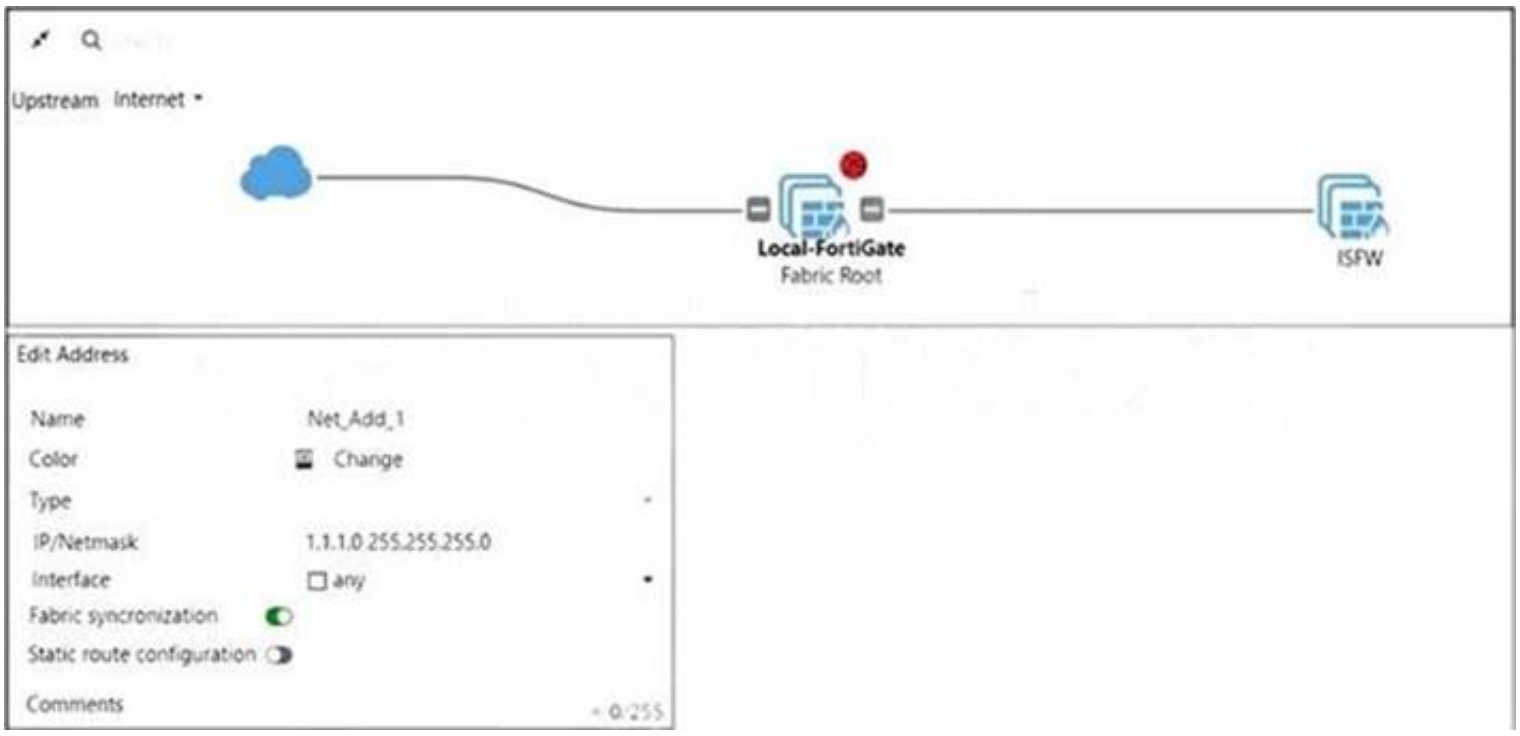


Exhibit B.

```
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 X18CtzrcUBUq9yz9nryP+YfM16
BJkv7S/trtoh2gYAe5CH8YMAa0GT18aX+/dKH/o5izw1ZEoN1QN2N
FGLT4r5z2AyYI8i1PxutiLcsCp1AdZadv1CxDe66IdLX7I6o22J9P
    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 sec configuration-sync local.
B. Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
C. Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion defaulc.
D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaulc.

Answer: A

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD43820

NEW QUESTION 32
- (Exam Topic 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

Answer: CD

NEW QUESTION 37
- (Exam Topic 1)
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. Application control is not enabled
B. SSL/SSH Inspection profile is incorrect
C. Antivirus profile configuration is incorrect
D. Antivirus definitions are not up to date

Answer: B

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

NEW QUESTION 39
- (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 43
- (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 46
- (Exam Topic 2)
Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.
B. The existing network IP schema must be changed when installing a transparent mode.
C. Static routes are required to allow traffic to the next hop.
D. FortiGate forwards frames without changing the MAC address.

Answer: AD

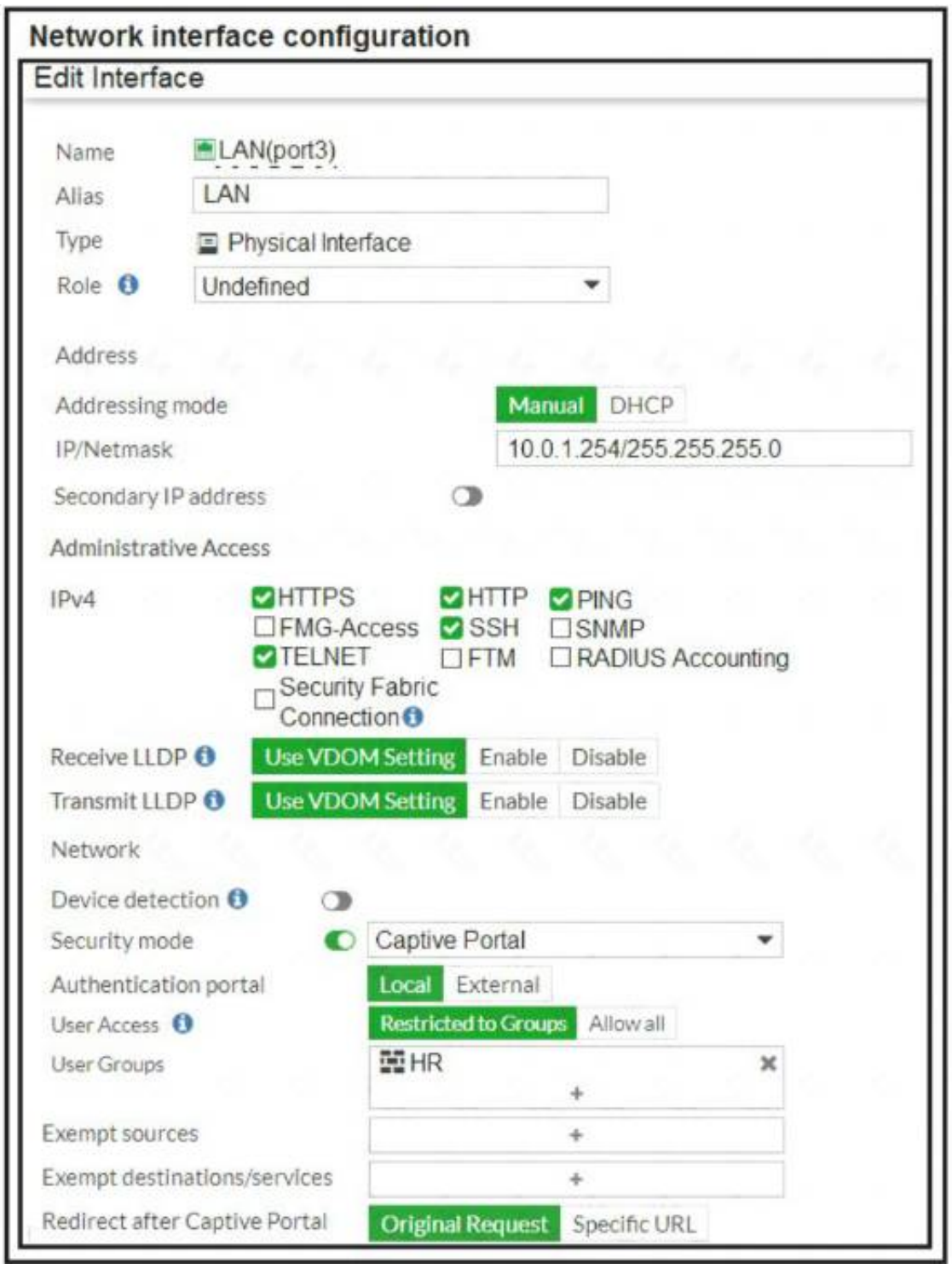
Explanation:
Reference: https://kb.fortinet.com/kb/viewAttachment.do?
attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

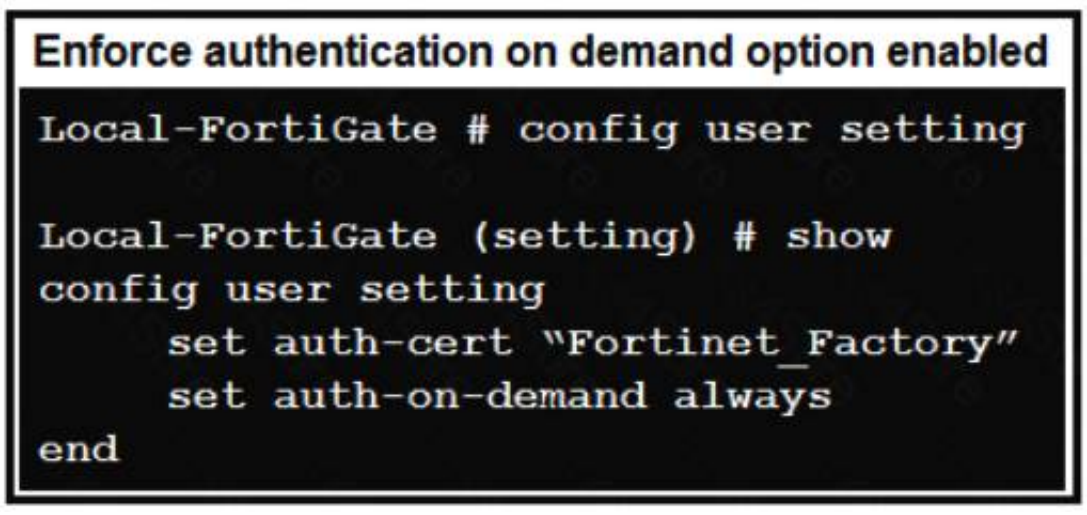
NEW QUESTION 49
- (Exam Topic 2)
An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

A. 192.168.3.0/24
B. 192.168.2.0/24
C. 192.168.1.0/24
D. 192.168.0.0/8

Answer: B

NEW QUESTION 51
- (Exam Topic 2)
Refer to the exhibit.





The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration. How will FortiGate handle user authentication for traffic that arrives on the LAN interface?

A. If there is a full-through policy in place, users will not be prompted for authentication.
B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.
C. Authentication is enforced at a policy level; all users will be prompted for authentication.
D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Answer: C

NEW QUESTION 55
- (Exam Topic 2)
Refer to the exhibit.

Which contains a network diagram and routing table output. The Student is unable to access Webserver.
What is the cause of the problem and what is the solution for the problem?

A. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
B. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
C. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.
D. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 203.0.114.24/32 through port3.

Answer: D

NEW QUESTION 56
- (Exam Topic 2)
FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.
Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning
B. File filter
C. DNS filter
D. Intrusion prevention

Answer: AD

NEW QUESTION 59
- (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 63
- (Exam Topic 2)
If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL
B. A person
C. A subordinate CA
D. A root CA

Answer: D

NEW QUESTION 66
- (Exam Topic 2)
Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

A. The subject field in the server certificate
B. The serial number in the server certificate

C. The server name indication (SNI) extension in the client hello message
D. The subject alternative name (SAN) field in the server certificate
E. The host field in the HTTP header

Answer: ACD

Explanation:
Reference: https://checkthefirewall.com/blogs/fortinet/ssl-inspection

NEW QUESTION 71
- (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?

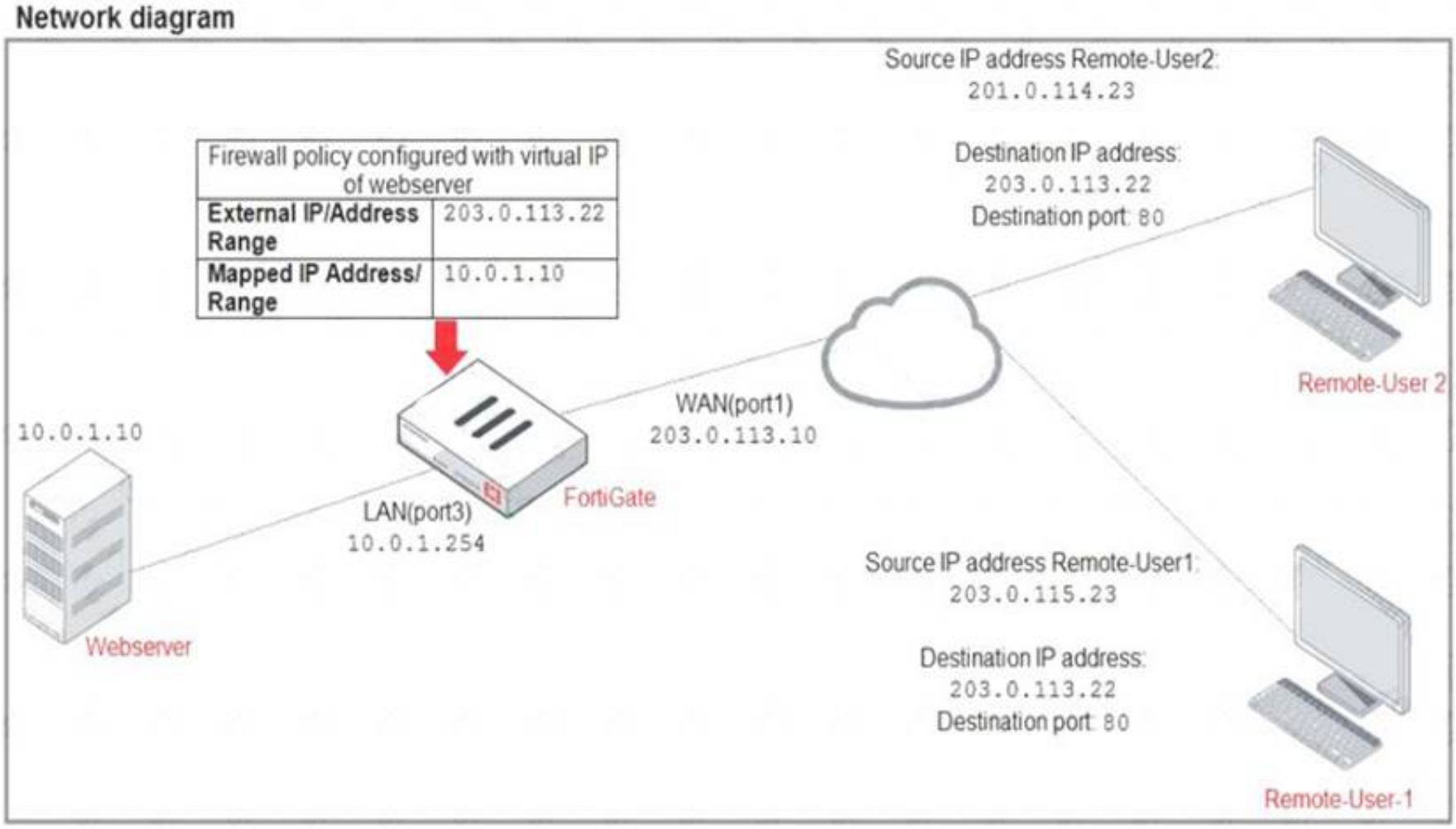
A. Log ID
B. Universally Unique Identifier
C. Policy ID
D. Sequence ID

Answer: B

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

NEW QUESTION 73
- (Exam Topic 2)
Refer to the exhibit.

Network diagram



ID	Name	Source	Destination	Schedule	Service	Action
WAN(port1) → LAN(port3) 2						
2	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Web_server	always	ALL	ACCEPT

The exhibit contains a network diagram, firewall policies, and a firewall address object configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-user2. Remote-user2 is still able to access Webserver.
Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.
B. Set the Destination address as Deny_IP in the Allow-access policy.
C. Enable match vip in the Deny policy.
D. Set the Destination address as Web_server in the Deny policy.

Answer: CD

NEW QUESTION 75
- (Exam Topic 2)
To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. FortiManager
B. Root FortiGate
C. FortiAnalyzer
D. Downstream FortiGate

Answer: B

NEW QUESTION 77
- (Exam Topic 2)
Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 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=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin ->sink: org pre->post, reply pre->post dev=5->3/3 ->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53 -> 10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e 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 statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.
B. The session is in TCP ESTABLISHED state.
C. The session is a bidirectional UDP connection.
D. The session is a bidirectional TCP connection.

Answer: C

NEW QUESTION 79
- (Exam Topic 2)
NGFW mode allows policy-based configuration for most inspection rules. Which security profile’s configuration does not change when you enable policy-based

inspection?

A. Web filtering
B. Antivirus
C. Web proxy
D. Application control

Answer: B

NEW QUESTION 83
- (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 86
- (Exam Topic 2)
Which of statement is true about SSL VPN web mode?

A. The tunnel is up while the client is connected.
B. It supports a limited number of protocols.
C. The external network application sends data through the VPN.
D. It assigns a virtual IP address to the client.

Answer: B

Explanation:
FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 88
- (Exam Topic 2)
Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password
B. FortiGate supports pre-shared key and signature as authentication methods.
C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.
D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Answer: AB

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticating-aremote-fortigate

NEW QUESTION 91
- (Exam Topic 2)
Refer to the exhibit to view the application control profile.

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

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

Answer: A

NEW QUESTION 93
- (Exam Topic 2)
Which two statements are true about collector agent standard access mode? (Choose two.)

A. Standard mode uses Windows convention-NetBios: Domain\Username.
B. Standard mode security profiles apply to organizational units (OU).
C. Standard mode security profiles apply to user groups.
D. Standard access mode supports nested groups.

Answer: AC

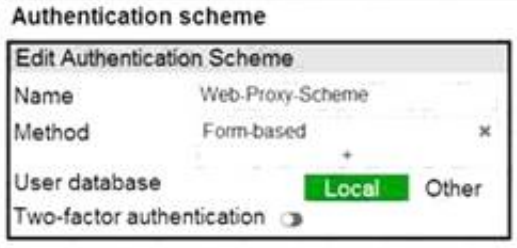
Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso

NEW QUESTION 94
- (Exam Topic 2)
Refer to the exhibit.

Authentication rule

Users

Authentication scheme

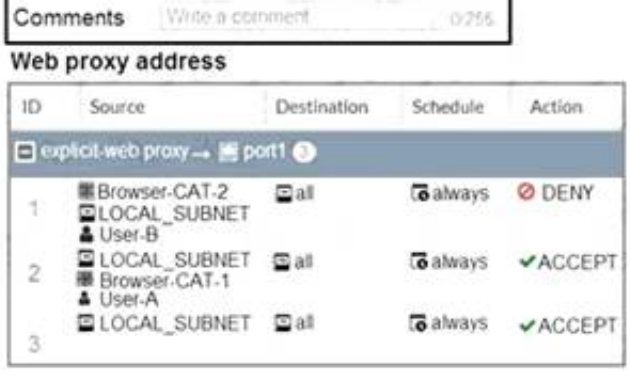


Firewall address

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 95
- (Exam Topic 2)
What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
B. FortiGate automatically negotiates a new security association after the existing security association expires.
C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=12069

NEW QUESTION 97
- (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 102
- (Exam Topic 2)
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries
B. PKI
C. Traffic shaping
D. DNS

Answer: AD

NEW QUESTION 106
- (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
```

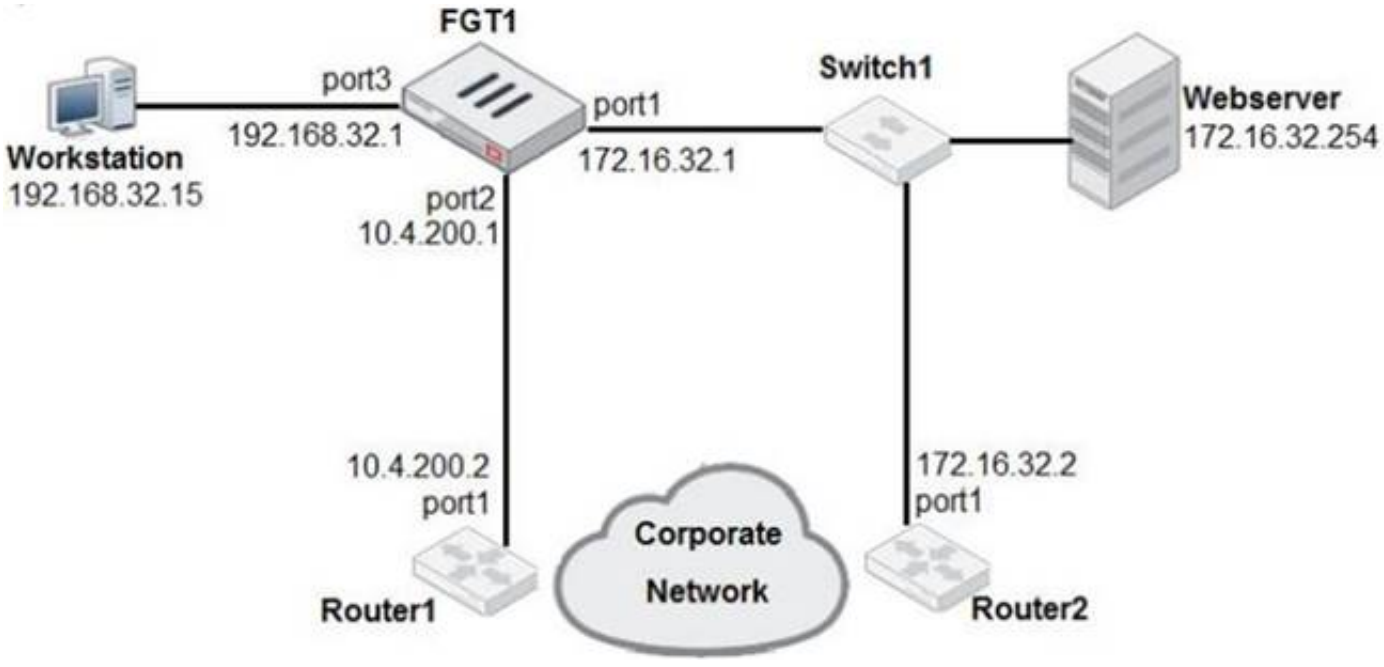
Refer to the exhibit to view the authentication rule configuration In this scenario, which statement is true?

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 110
- (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 113
- (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 115
- (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 116
- (Exam Topic 2)
In which two ways can RPF checking be disabled? (Choose two)

A. Enable anti-replay in firewall policy.
B. Disable the RPF check at the FortiGate interface level for the source check
C. Enable asymmetric routing.
D. Disable strict-arc-check under system settings.

Answer: CD

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

NEW QUESTION 117
- (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 122
- (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 124
- (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 128
- (Exam Topic 2)
Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

A. Fabric Coverage
B. Automated Response
C. Security Posture
D. Optimization

Answer: C

Explanation:
Reference:
https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-bestpractices.pdf

NEW QUESTION 131
- (Exam Topic 2)
A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser
does not report errors.
What is the reason for the certificate warning errors?

A. The browser requires a software update.
B. FortiGate does not support full SSL inspection when web filtering is enabled.
C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
D. There are network connectivity issues.

Answer: C

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394

NEW QUESTION 133
- (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 135
- (Exam Topic 2)
Refer to the exhibit.

FIREWALL POLICIES

```
config firewall policy
    edit 1
        set name "INTERNET"
        set uuid b11ac58c-791b-51e7-4600-12f829a689d9
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "LOCAL_SUBNET"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set inspection-mode proxy
        set http-policy-redirect enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set logtraffic all
        set logtraffic-start enable
        set ippool enable
        set poolname "ProxyPool"
        set nat enable
    next
end
```

PROXY ADDRESS

```
config firewall proxy-address
    edit "EICAR"
        set uuid 5a24bdaa-c792-51ea-2c89-a9f79e2bdc96
        set type host-regex
        set host-regex ".*eicar\\.org"
    next
end
```

```
config firewall
    edit 1
        set uuid 6491d126-c790-51ea-13f9-4ed04b543a8e
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "EICAR"
        set service "webproxy"
        set action accept
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
    next
    edit 2
        set uuid 6a1c74c6-c794-51ea-e646-4f70ae2bc5f9
        set proxy transparent-web
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set status disable
        set schedule "always"
        set logtraffic disable
        set ssl-ssh-profile "certificate-inspection"
    next
    edit 3
        set uuid 818fb8b6-c797-51ea-d848-a7c2952ceea9
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set service "webproxy"
        set action accept
        set status disable
        set schedule "always"
        set logtraffic all
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
    next
end
```

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 139
- (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

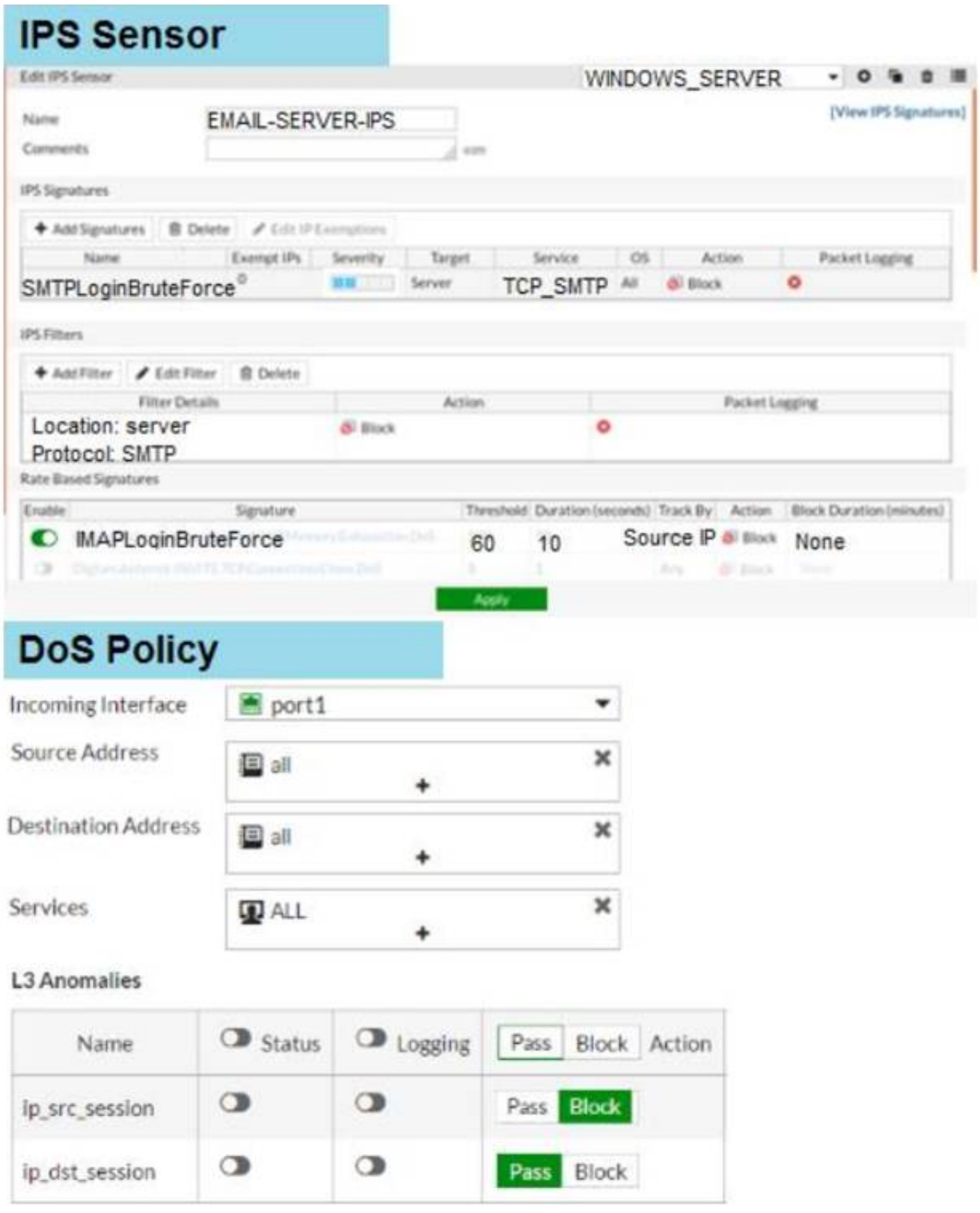
Answer: A

NEW QUESTION 143
- (Exam Topic 2)
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.
B. By default, the SSL VPN portal requires the installation of a client's certificate.
C. By default, split tunneling is enabled.
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 148
- (Exam Topic 2)
Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.



When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

A. SMTP.Login.Brute.Force
B. IMAP.Login.brute.Force
C. ip_src_session
D. Location: server Protocol: SMTP

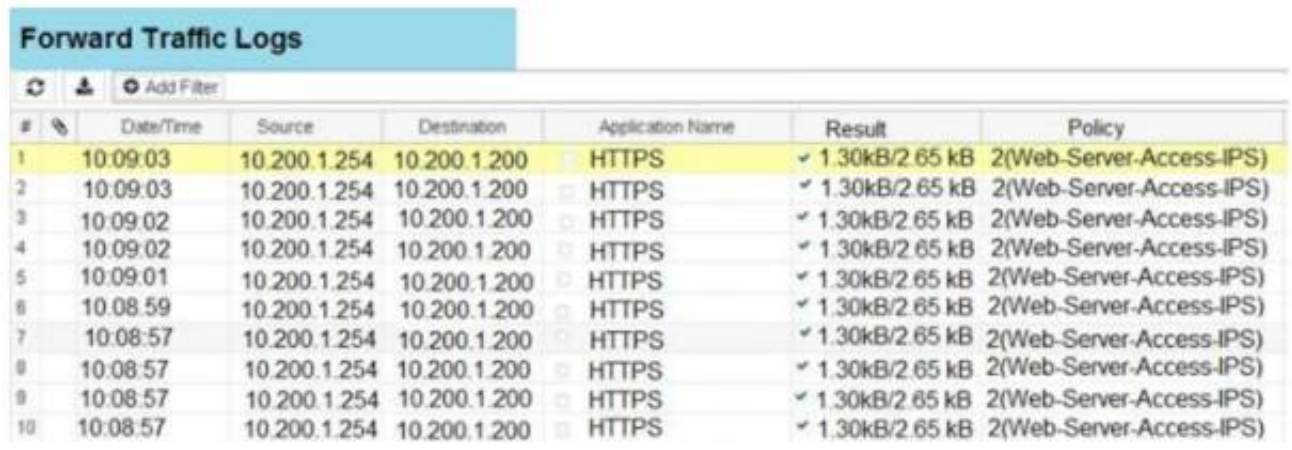
Answer: B

NEW QUESTION 151
- (Exam Topic 2)
Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeou
B. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source IP.
C. It is a hard timeou
D. The FortiGate removes the temporary policy for a user’s source IP address after this timer has expired.
E. It is an idle timeou
F. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source MAC.
G. It is a hard timeou
H. The FortiGate removes the temporary policy for a user’s source MAC address after this timer has expired.

Answer: A

NEW QUESTION 153
- (Exam Topic 2)
Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.



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?

A. The IPS filter is missing the Protocol: HTTPS option.
B. The HTTPS signatures have not been added to the sensor.
C. A DoS policy should be used, instead of an IPS sensor.
D. A DoS policy should be used, instead of an IPS sensor.
E. The firewall policy is not using a full SSL inspection profile.

Answer: E

NEW QUESTION 155
- (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 159
- (Exam Topic 2)
Which two statements ate true about the Security Fabric rating? (Choose two.)

A. It provides executive summaries of the four largest areas of security focus.
B. Many of the security issues can be fixed immediately by clicking Apply where available.
C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
D. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.

Answer: BC

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/292634/security-rating

NEW QUESTION 160
- (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 161
- (Exam Topic 2)
Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

A. Heartbeat interfaces have virtual IP addresses that are manually assigned.
B. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
C. Virtual IP addresses are used to distinguish between cluster members.
D. The primary device in the cluster is always assigned IP address 169.254.0.1.

Answer: BD

NEW QUESTION 163
- (Exam Topic 2)
Examine this output from a debug flow:

```
id=20085 trace_id=1 func=print_pkt_detail line=5363 msg="vd-root received a packet(proto=1,
10.0.1.10:1->10.200.1.254:2048)
from port3. type=8, code=0, id=1, seq=33."
id=20085 trace_id=1 func=init_ip_session_common line=5519 msg="allocate a new session=00000340"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2583 msg="find a route: flag=04000000 gw=10.200.1.254 via
port1"
id=20085 trace_id=1 func=fw_forward_handler line=586 msg="Denied by forward policy check (policy 0)"
```

Why did the FortiGate drop the packet?

A. The next-hop IP address is unreachable.
B. It failed the RPF check.
C. It matched an explicitly configured firewall policy with the action DENY.
D. It matched the default implicit firewall policy.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=13900

NEW QUESTION 166
- (Exam Topic 2)
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?

A. It is allowed, but with no inspection
B. It is allowed and inspected as long as the inspection is flow based
C. It is dropped.

D. It is allowed and inspected, as long as the only inspection required is antivirus.

Answer: C

NEW QUESTION 171
- (Exam Topic 2)
An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway.
What must an administrator do to achieve this objective?

A. The administrator can register the same FortiToken on more than one FortiGate.
B. The administrator must use a FortiAuthenticator device.
C. The administrator can use a third-party radius OTP server.
D. The administrator must use the user self-registration server.

Answer: B

NEW QUESTION 174
- (Exam Topic 2)
Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.
B. Only secondary FortiGate devices are rebooted.
C. Uninterruptable upgrade is enabled by default.
D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 175
- (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 178
- (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 180
- (Exam Topic 2)
How do you format the FortiGate flash disk?

A. Load a debug FortiOS image.
B. Load the hardware test (HQIP) image.
C. Execute the CLI command execute formatlogdisk.
D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 183
- (Exam Topic 2)
What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

A. Full Content inspection
B. Proxy-based inspection
C. Certificate inspection
D. Flow-based inspection

Answer: D

NEW QUESTION 187
.....

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