Fortinet

Exam Questions NSE4_FGT-6.4

Fortinet NSE 4 - FortiOS 6.4

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Traffic to botnetservers
B. Traffic to inappropriate web sites
C. Server information disclosure attacks
D. Credit card data leaks
E. SQL injection attacks

Answer: ACE

NEW QUESTION 2
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

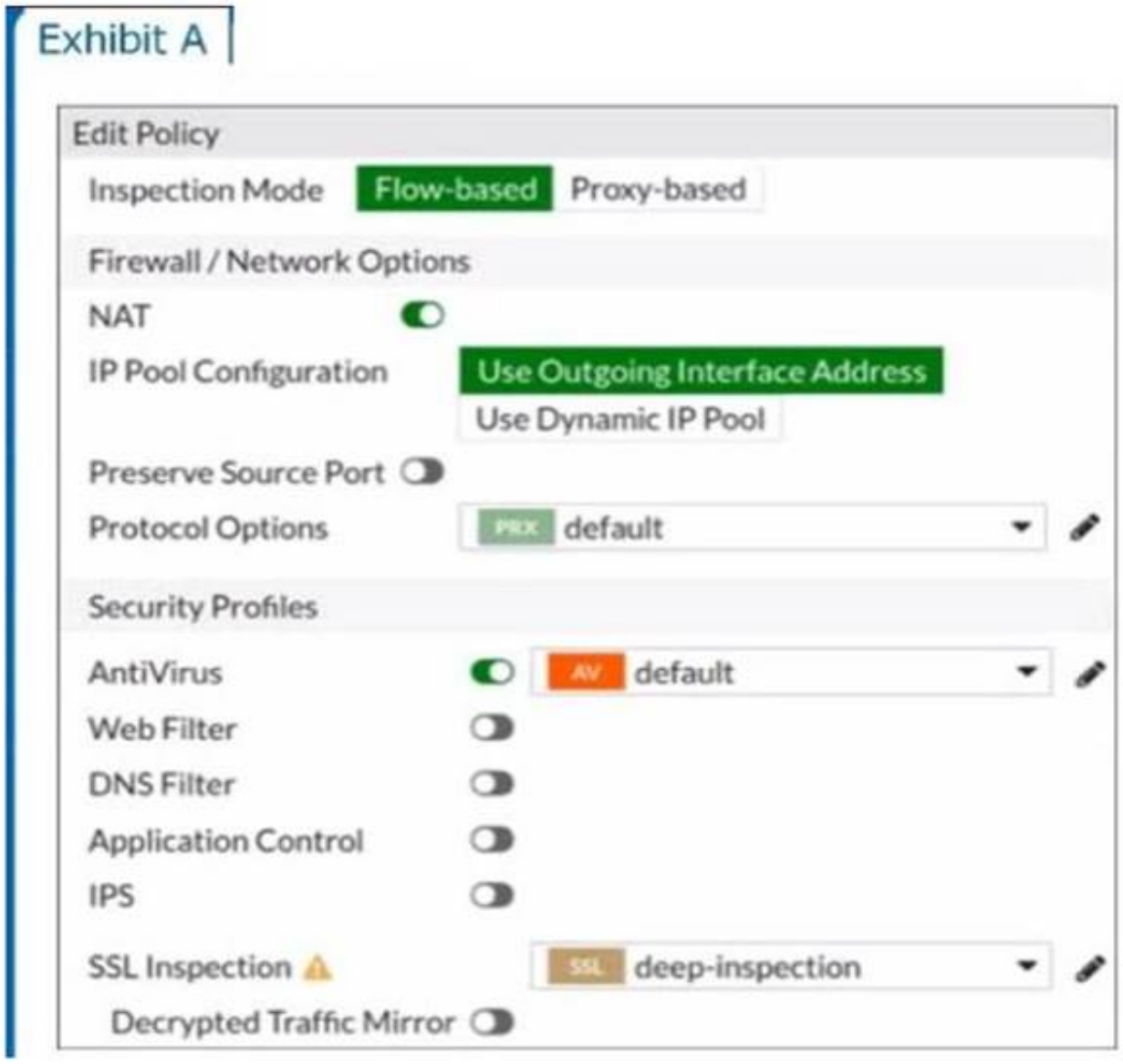
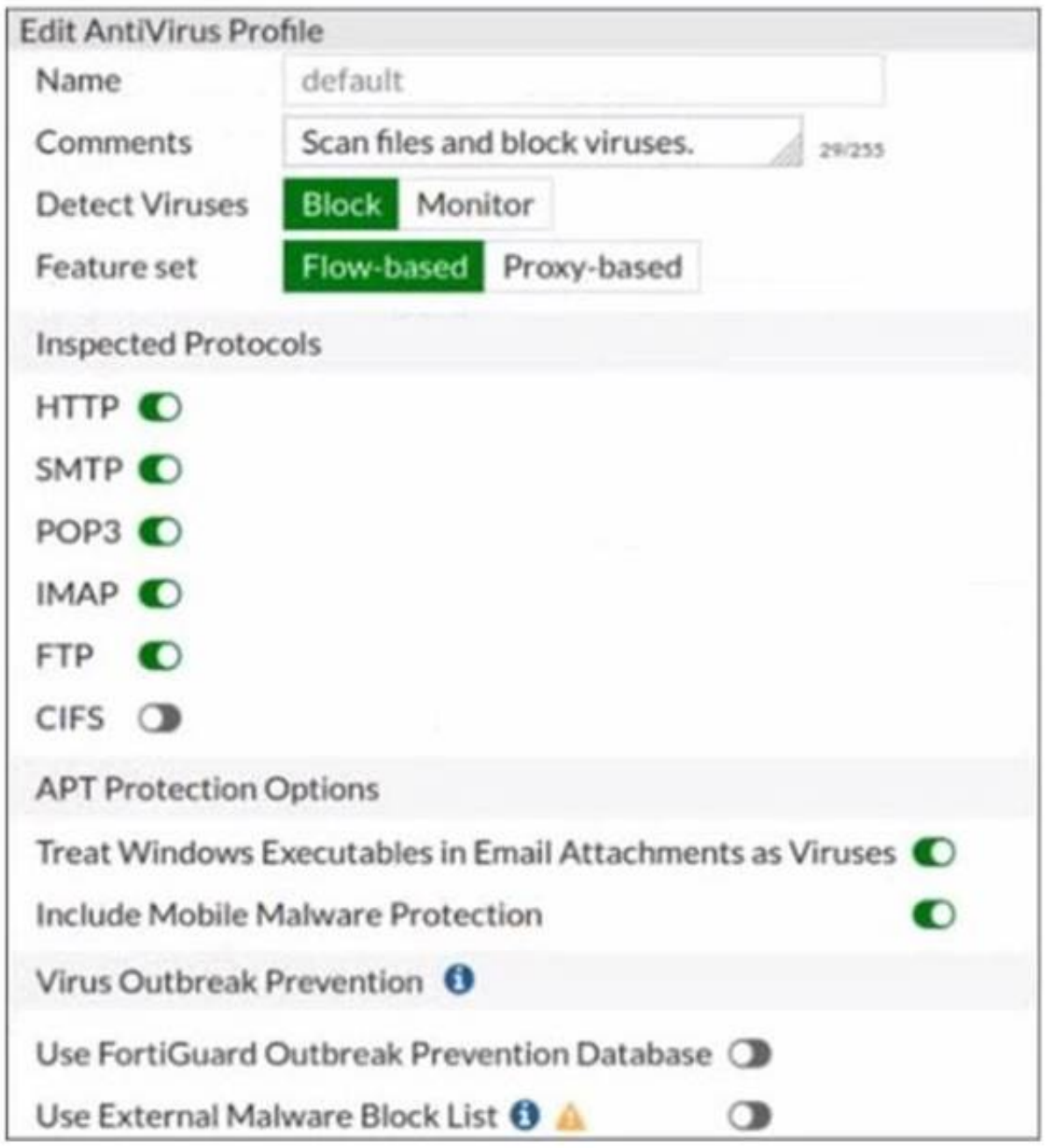


Exhibit B



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: A

NEW QUESTION 3
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 4
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 befixed immediately by click ng 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: AC

NEW QUESTION 5
Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
B. An SA never expires.
C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
D. Phase 2 SA expiration can be time-based, volume-based, or both.
E. Both the phase 1 SA and phase 2 SA are bidirectional.

Answer: BCD

NEW QUESTION 6
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

A. diagnose wad session list
B. diagnose wad session list | grep hook-pre&&hook-out
C. diagnose wad session list | grep hook=pre&&hook=out
D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: D

NEW QUESTION 7
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: C

NEW QUESTION 8
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 9
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 10
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 10
A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface.
Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
B. The two VLAN sub interfaces must have different VLAN IDs.
C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

Answer: B

Explanation:
FortiGate_Infrastructure_6.0_Study_Guide_v2-Online.pdf –> page 147
“Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID”

NEW QUESTION 11
Refer to the exhibit.

Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

A. This security fabric topology is a logical topology view.
B. There are 19 security recommendations for the security fabric.
C. There are five devices that are part of the security fabric.
D. Device detection is disabled on all FortiGate devices.

Answer: AD

NEW QUESTION 13
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: BD

NEW QUESTION 17
Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?

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

Answer: B

NEW QUESTION 21

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 sourceusingtheincoming 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.

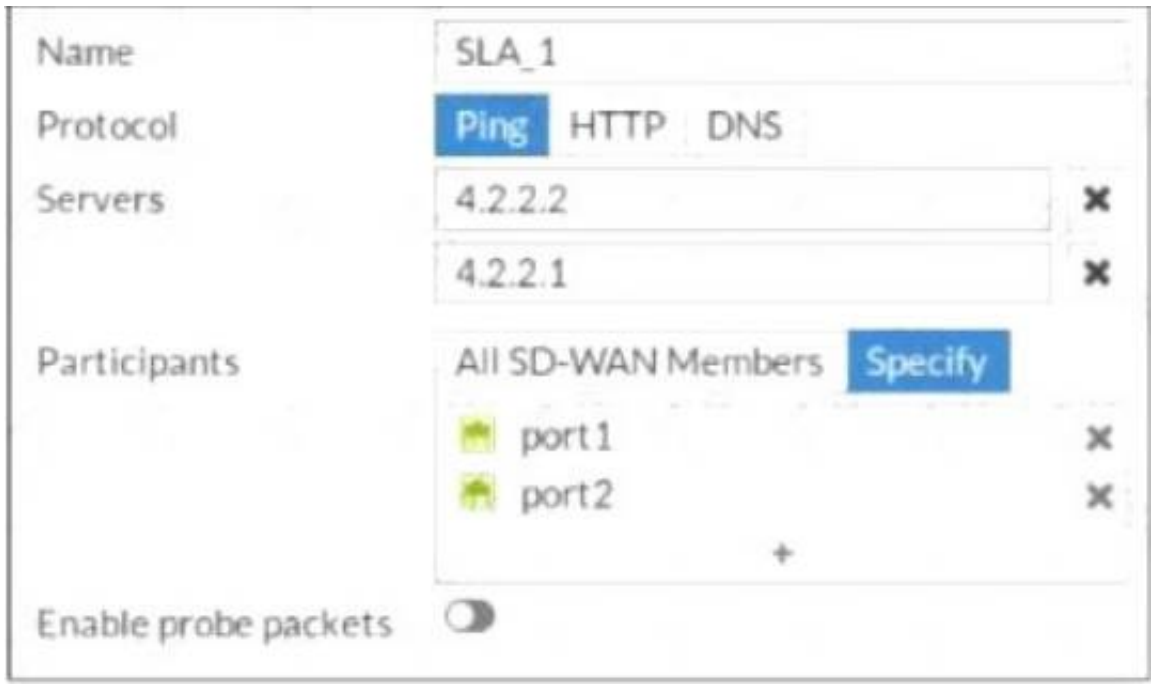
Answer: A

NEW QUESTION 22
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: C

NEW QUESTION 26
Refer to the exhibit.



Which contains a PerformanceSLA configuration.
An administrator has configured a performance SLA on FortiGate. Which failed to generate any traffic. Why is FortiGate not generating any traffic for the performance SLA?

A. Participants configured are not SD-WAN members.
B. There may not be a static route to route the performance SLA traffic.
C. The Ping protocol is not supported for the public servers that are configured.
D. You need to turn on the Enable probe packets switch.

Answer: D

NEW QUESTION 27
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: A

NEW QUESTION 28
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
```

PROXY POLICIES

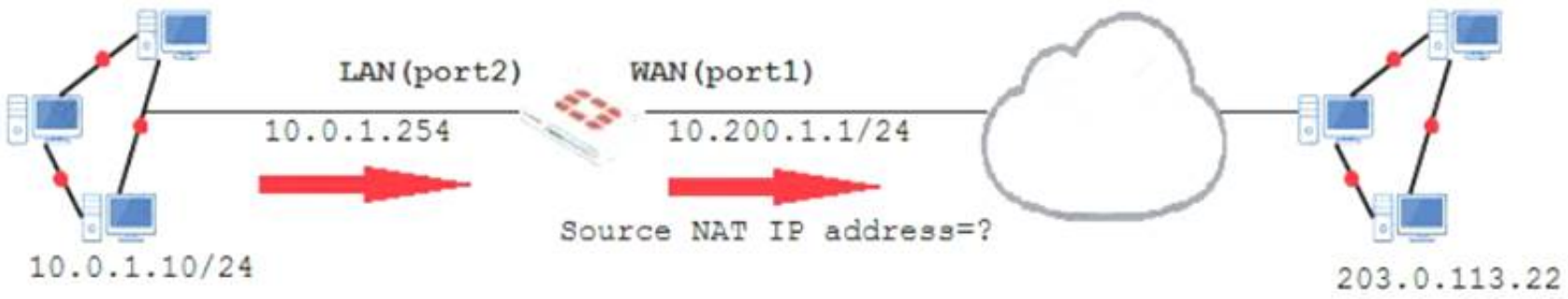
```
config firewall
    edit 1
        set uuid 04f91d12b-c790-51ea-13f9-4ad04b543a0e
        set proxy transparent-web
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "EICAR"
        set service "webproxy"
        set action accept
        set schedule "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
```

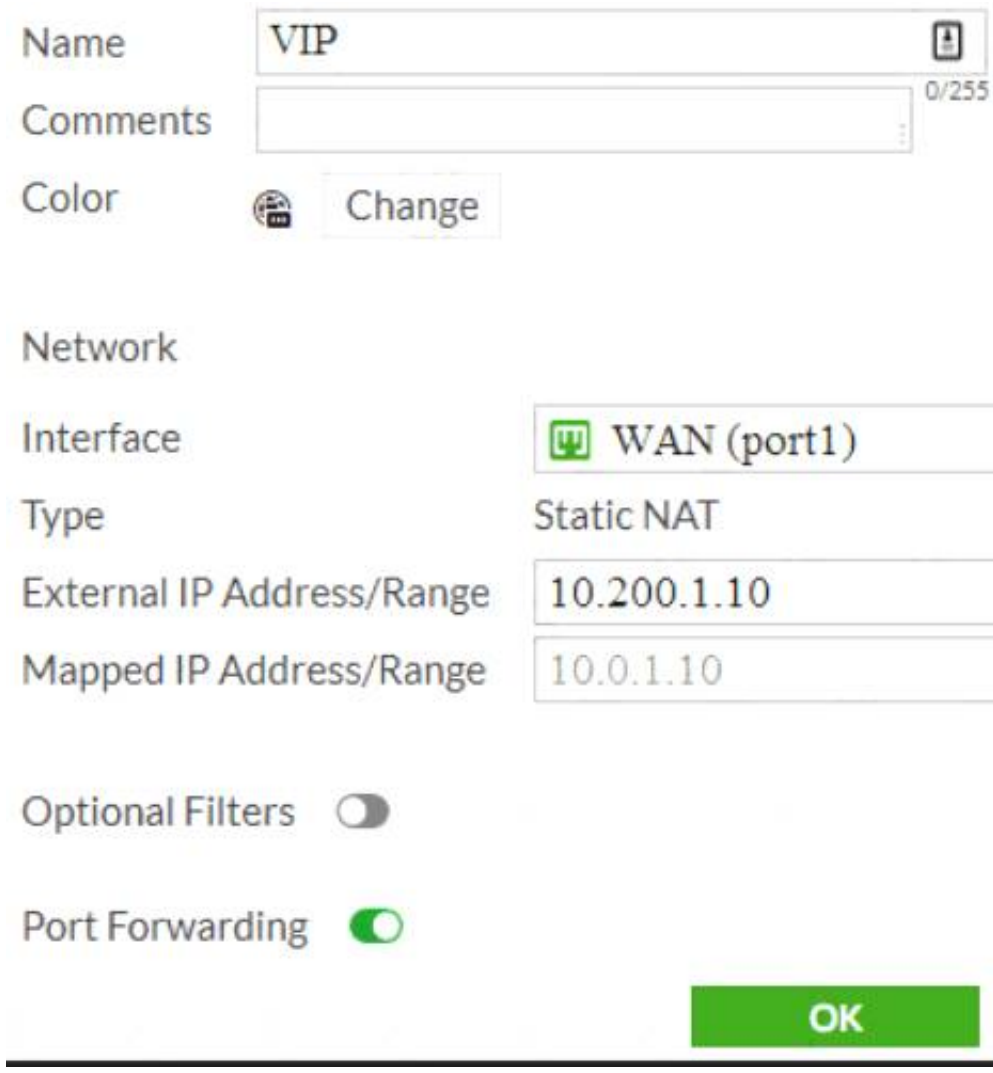
The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.
How does FortiGate process the traffic sent to http://www.fortinet.com?

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 32
Examine the exhibit, which contains a virtual IP and firewall policy configuration.





The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port2) interface has the IP address 10.0.1.254/24.
The first firewall policy has NAT enabled on the outgoing interface address. The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0.1.10/24?

A. 10.200.1.10
B. Any available IP address in the WAN (port1) subnet 10.200.1.0/24
C. 10.200.1.1
D. 10.0.1.254

Answer: B

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs.

NEW QUESTION 34
Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

A. FortiGate points the collector agent to use a remote LDAP server.
B. FortiGate uses the AD server as the collector agent.
C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
D. FortiGate queries AD by using the LDAP to retrieve user group information.

Answer: CD

NEW QUESTION 38
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?

A. The public key of the web servercertificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The CA certificate that signed the web-server certificate must be installed on the browser.
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Answer: C

NEW QUESTION 43
Which two statements are true about the FGCP protocol? (Choose two.)

A. Not used when FortiGate is in Transparent mode
B. Elects the primary FortiGate device
C. Runs only over the heartbeat links
D. Is used to discover FortiGate devices in different HA groups

Answer: CD

NEW QUESTION 47
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: A

NEW QUESTION 48
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.
D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: AC

NEW QUESTION 53
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_SEXT 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: D

NEW QUESTION 56
Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.
Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.
B. The IPS engine was unable to prevent an intrusion attack.
C. The IPS engine was blocking all traffic.
D. The IPS engine will continue to run in a normal state.

Answer: C

NEW QUESTION 61
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent must search security event logs.
D. The NetSessionEnum functionis user] to track user logouts.

Answer: A

NEW QUESTION 66
If theServicesfield is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

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

Answer: C

NEW QUESTION 69
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 71
Refer to theexhibits.

Exhibit A

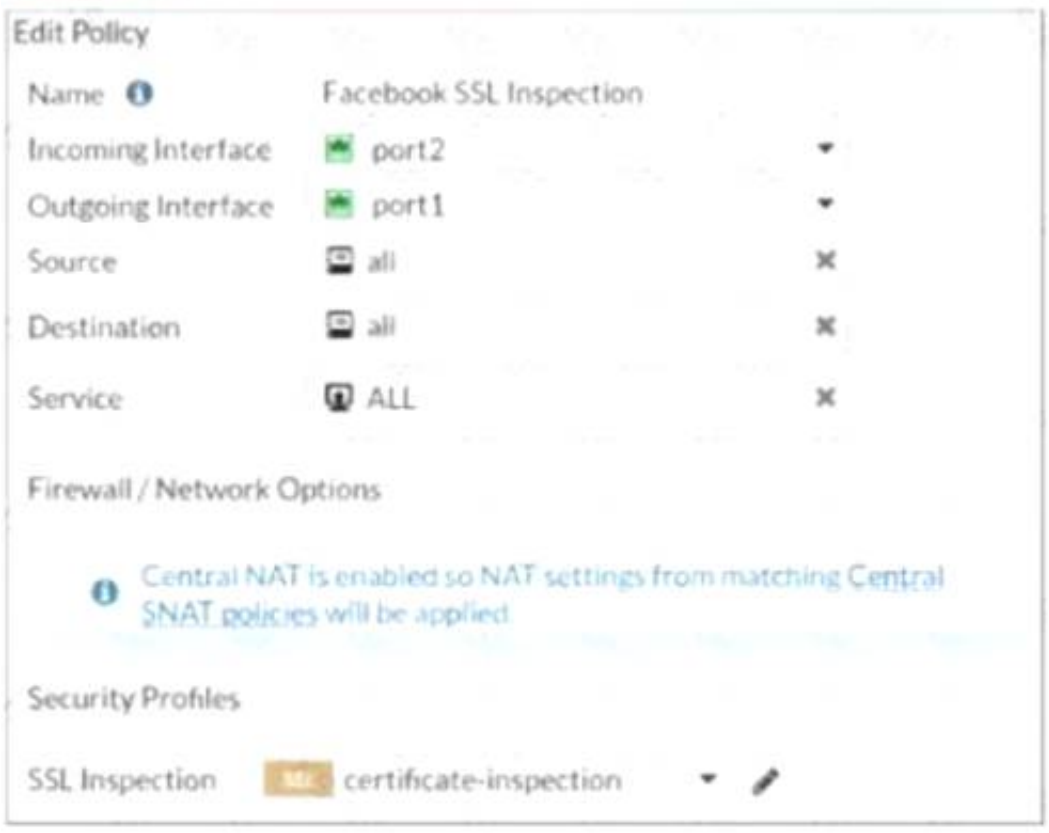


Exhibit B

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 areunableto leavereactions on videos or other types ofposts.
Which part ofthe policy configuration must you change to resolve the issue?

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

Answer: A

NEW QUESTION 75
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 80
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: C

NEW QUESTION 84
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. A.-192.168.3.0/24B.192.168.2.0/24C.192.168.1.0/24D.192.168.0.0/8

Answer: B

NEW QUESTION 86
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 87
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: D

NEW QUESTION 88
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?

A. Add the support of NTLM authentication.
B. Add useraccounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Answer: C

NEW QUESTION 93
Examine this FortiGate configuration:

```
config authentication setting
     set active-auth-scheme SCHEME1
end
config authentication rule
     edit WebProxyRule
       set srcaddr 10.0.1.0/24
       set active-auth-method SCHEME2
     next
end
```

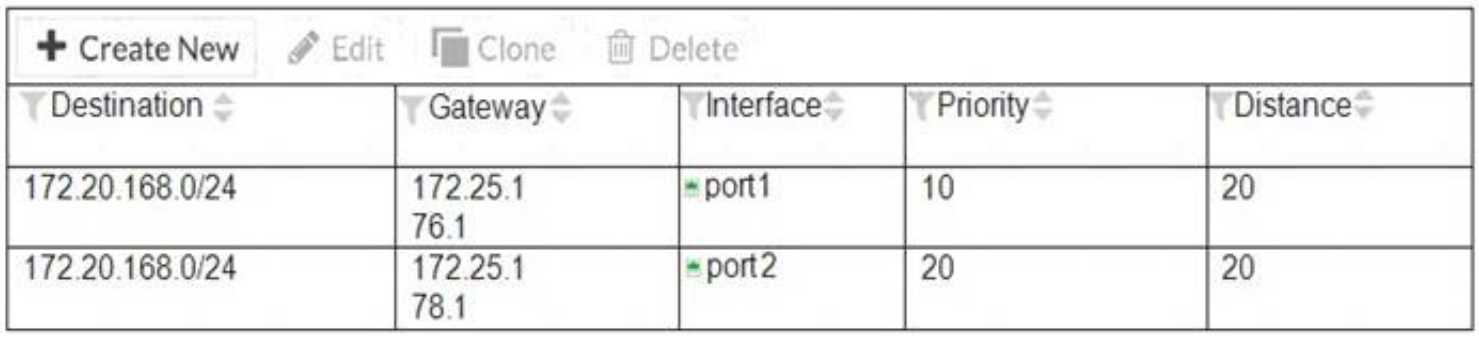
How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.
B. It drops the traffic.
C. It authenticates the traffic using the authentication scheme SCHEME2.
D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:
“What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting”

NEW QUESTION 98
Examine the two static routes shown in the exhibit, then answer the following question.



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 99
An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

Answer: ABC

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

NEW QUESTION 100
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 103
.....

Relate Links

100% Pass Your NSE4_FGT-6.4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-6.4-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/