Fortinet.NSE4_FGT-6.4.v2022-05-20.q136

Exam Code:	NSE4_FGT-6.4
Exam Name:	Fortinet NSE 4 - FortiOS 6.4
Certification Provider:	Fortinet
Free Question Number:	136
Version:	v2022-05-20
# of views:	4337
# of Questions views:	1360
https://www.exam-tests.com/NSE4_FGT-6.4-exam/Fortinet.NSE4_FGT-6.4.v2022-05-20.q136.html	

NEW QUESTION: 1
Which two statements are correct about SLA targets? (Choose two.)
A. SLA targets are used only when referenced by an SD-WAN rule.
B. SLA targets are optional.
C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
D. You can configure only two SLA targets per one Performance SL
Answer: (SHOW ANSWER)

NEW QUESTION: 2
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 (LEAVE A REPLY)
"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: 3

Which three statements about a flow-based antivirus profile are correct? (Choose three.)

A. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

B. FortiGate buffers the whole file but transmits to the client simultaneously.

C. If the virus is detected, the last packet is delivered to the client.

D. IPS engine handles the process as a standalone.

E. Optimized performance compared to proxy-based inspection.

Answer: (SHOW ANSWER)

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 be fixed 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: (SHOW ANSWER)

FortiGate_Security_6.4_Study_Guide-Online. page 89

NEW QUESTION: 5

Refer to the exhibit.

```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
orgin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

A. The session is in SYN_SENT state.

B. The session is in FIN_ACK state.

C. The session is in FTN_WAIT state.

D. The session is in ESTABLISHED state.

Answer: A (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 6
Refer to the web filter raw logs.

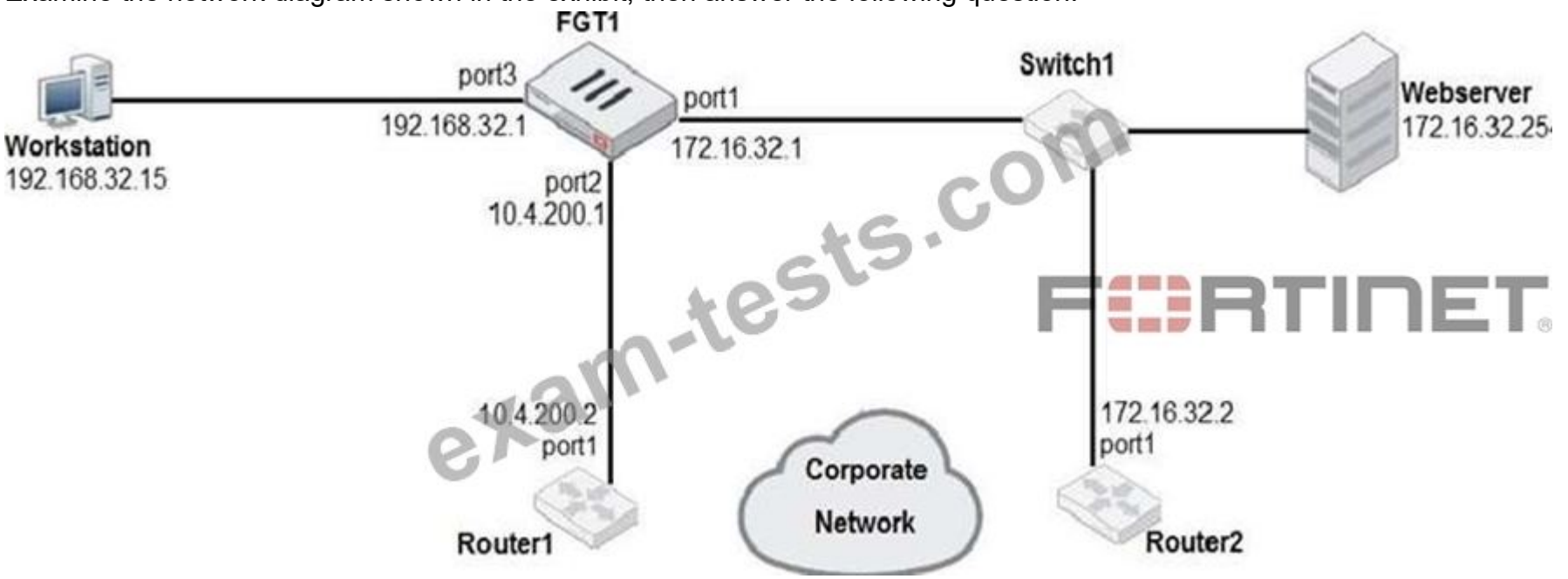
Based on the raw logs shown in the exhibit, which statement is correct?
A. The name of the firewall policy is all_users_web.
B. Access to the social networking web filter category was explicitly blocked to all users.
C. The action on firewall policy ID 1 is set to warning.
D. Social networking web filter category is configured with the action set to authenticate.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
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 CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
B. There are network connectivity issues.
C. FortiGate does not support full SSL inspection when web filtering is enabled.
D. The browser requires a software update.
Answer: (SHOW ANSWER)

NEW QUESTION: 8

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 Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.
B. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
C. The IP version of the sources and destinations in a firewall policy must be different.
D. The IP version of the sources and destinations in a policy must match.
E. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
B. 10.4.200.0/30 is directly connected, port2
C. 172.16.32.0/24 is directly connected, port1
D. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
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: B,D,E (LEAVE A REPLY)

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

NEW QUESTION: 11

Refer to the exhibit.

Why did FortiGate drop the packet?

A. It matched an explicitly configured firewall policy with the action DENY.

B. The next-hop IP address is unreachable.

C. It failed the RPF check.

D. It matched the default implicit firewall policy.

Answer: B (LEAVE A REPLY)

Explanation/Reference:

https://www.fast2test.com/NSE4_FGT-6.4-practice-test.html 14

Valid Fast2test NSE4_FGT-6.4 Exam PDF Dumps - New NSE4_FGT-6.4 Real Exam Questions

NEW QUESTION: 12

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. Traffic matching the signature will be silently dropped and logged.

B. The signature setting uses a custom rating threshold.

C. The signature setting includes a group of other signatures.

D. Traffic matching the signature will be allowed and logged.

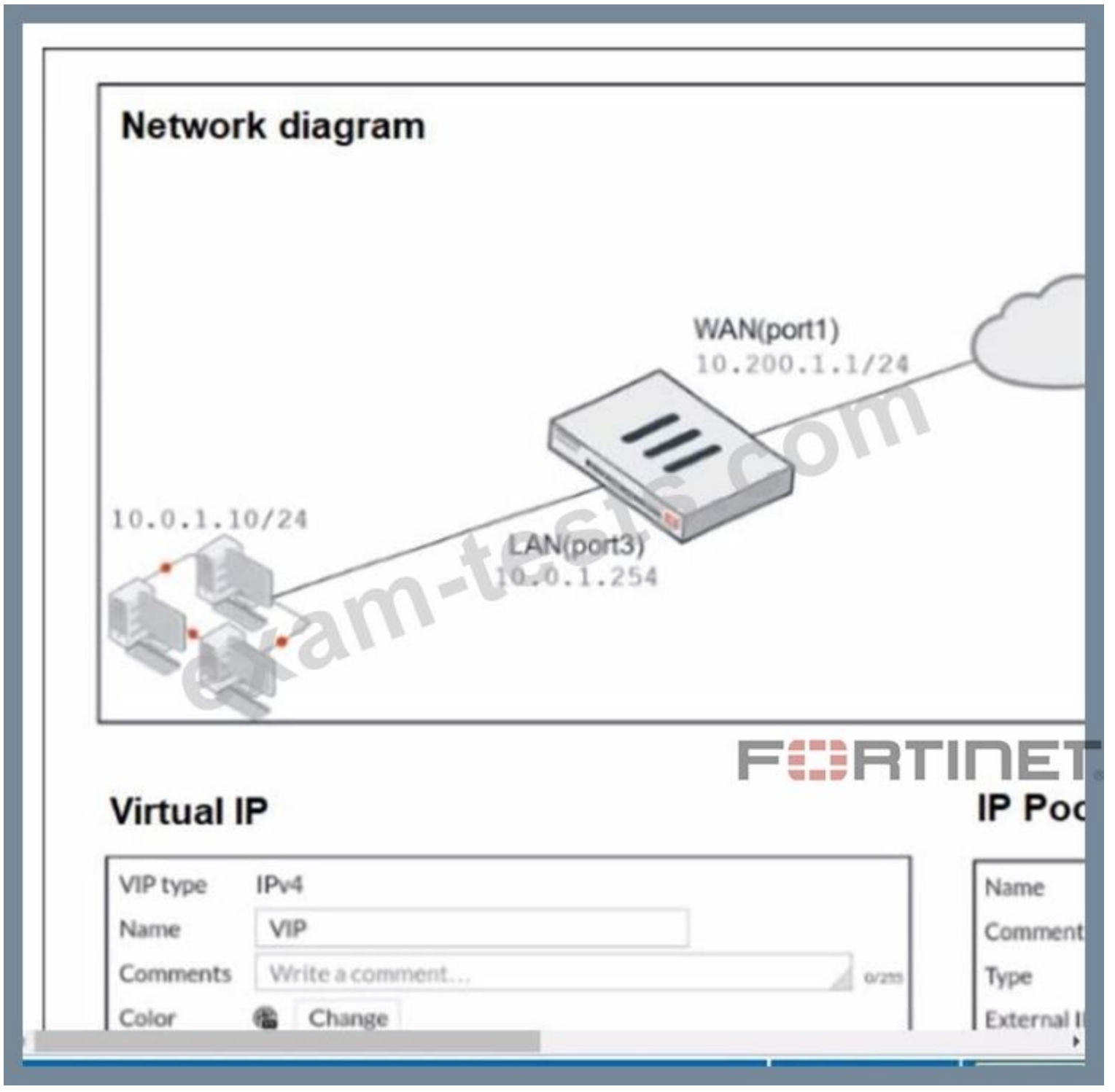
Answer: D (LEAVE A REPLY)

NEW QUESTION: 13
What devices form the core of the security fabric?
A. One FortiGate device and one FortiManager device
B. One FortiGate device and one FortiAnalyzer device
C. Two FortiGate devices and one FortiManager device
D. Two FortiGate devices and one FortiAnalyzer device
Answer: (SHOW ANSWER)

NEW QUESTION: 14
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 192.160.1.0/24 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. 192.168.3.0/24
B. 192.168.1.0/24
C. 192.168.2.0/24
D. 192.168.0.0/24
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
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 single
Answer: C (LEAVE A REPLY)
computer.

NEW QUESTION: 16
Refer to the exhibit.



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

The WAN (port1) interface has the IP address 10.200.1.1/24.

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

The first firewall policy has NAT enabled using IP Pool.

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

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

A. 10.200.1.10

B. 10.200.1.1

C. 10.200.3.1

D. 10.200.1.100

Answer: (SHOW ANSWER)

NEW QUESTION: 17

Examine this output from a debug flow:

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: (SHOW ANSWER)

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

NEW QUESTION: 18

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. Read/Write permission for Log & Report

B. Read/Write permission for Firewall

C. Custom permission for Network

D. CLI diagnostics commands permission
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
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. DNS
D. NTP
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 20
How does FortiGate act when using SSL VPN in web mode?
A. FortiGate acts as an FDS server.
B. FortiGate acts as an HTTP reverse proxy.
C. FortiGate acts as DNS server.
D. FortiGate acts as router.
Answer: C (LEAVE A REPLY)
Explanation/Reference: https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate- sslvpn-40-mr3.pdf

NEW QUESTION: 21
Refer to the exhibits.

Exhibit A | Exhibit B

```
# 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%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 0 / 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
```

Exhibit A | Exhibit B

```
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.)

A. Administrators can access FortiGate only through the console port.
B. FortiGate has entered conserve mode.
C. FortiGate will start sending all files to FortiSandbox for inspection.
D. Administrators cannot change the configuration.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 22
Refer to the exhibits.

Exhibit A | Exhibit B

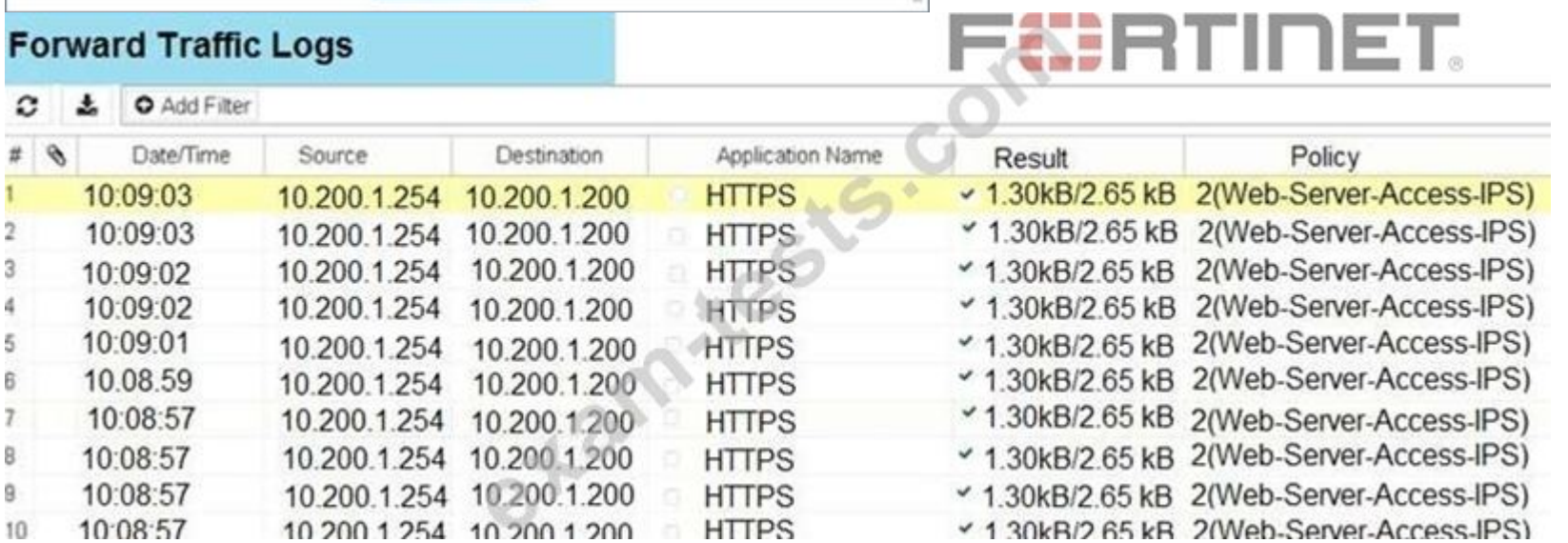
```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 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
```

Exhibit A | Exhibit B

```
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.)
A. FortiGate will start sending all files to FortiSandbox for inspection.
B. Administrators can access FortiGate only through the console port.
C. Administrators cannot change the configuration.
D. FortiGate has entered conserve mode.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 23
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 firewall policy is not using a full SSL inspection profile.

B. The IPS filter is missing the Protocol: HTTPS option.

C. The HTTPS signatures have not been added to the sensor.

D. A DoS policy should be used, instead of an IPS sensor.

E. A DoS policy should be used, instead of an IPS sensor.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 24

Which two statements ate true about the Security Fabric rating? (Choose two.)

A. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.

B. Many of the security issues can be fixed immediately by click ng Apply where available.

C. It provides executive summaries of the four largest areas of security focus.

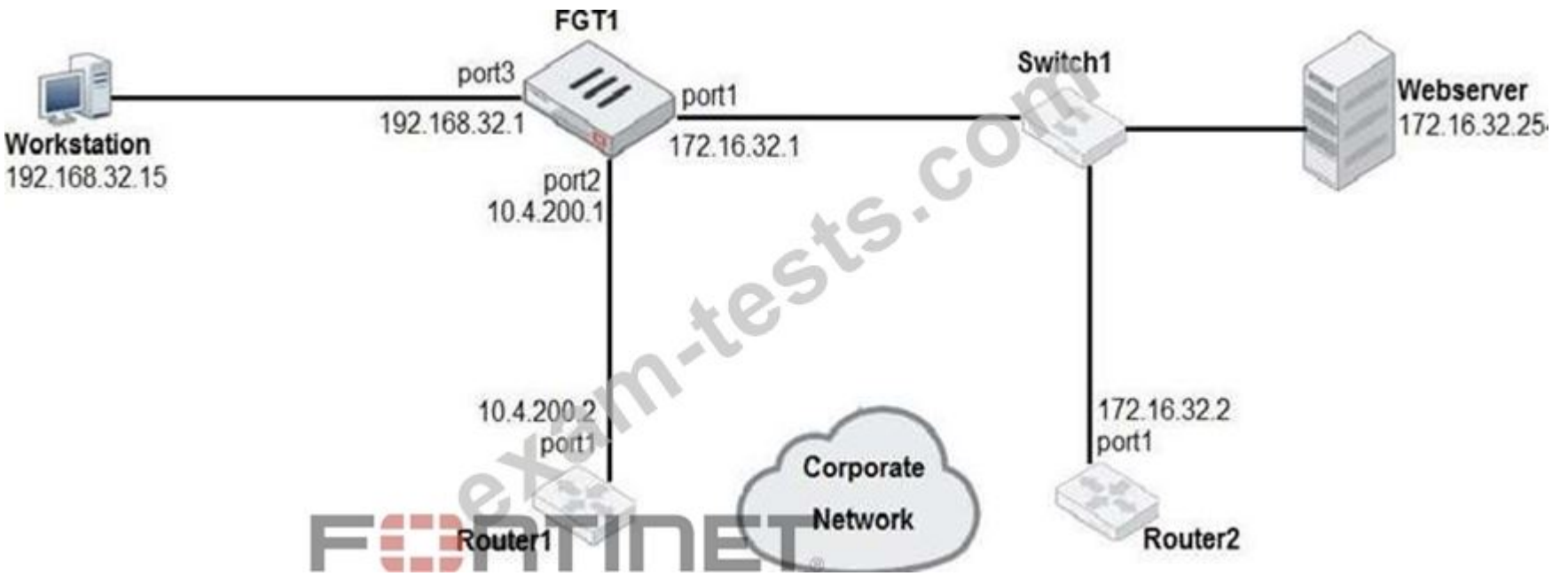
D. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 25
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?
A. It limits the scanning of application traffic to use parent signatures only.
B. It limits the scanning of application traffic to the browser-based technology category only.
C. It limits the scanning of application traffic to the DNS protocol only.
D. It limits the scanning of application traffic to the application category only.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)
A. Policy rule
B. Firewall policy
C. SSL inspection and authentication policy
D. Security policy
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 27
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 (LEAVE A REPLY)
Explanation
In a route-based configuration, FortiGate automatically adds a virtual interface eith the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION: 28
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 (LEAVE A REPLY)

NEW QUESTION: 29

Refer to the exhibit.

```
STUDENT # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT        DESTINATION       DESTINATION-NAT
tcp     3598   10.0.1.10:2706  10.200.1.6:2706   10.0.1.254:80     -
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?

A. One-to-one NAT IP pool is used in the firewall policy.

B. Destination NAT is disabled in the firewall policy.

C. Overload NAT IP pool is used in the firewall policy.

D. Port block allocation IP pool is used in the firewall policy.

Answer: B (LEAVE A REPLY)

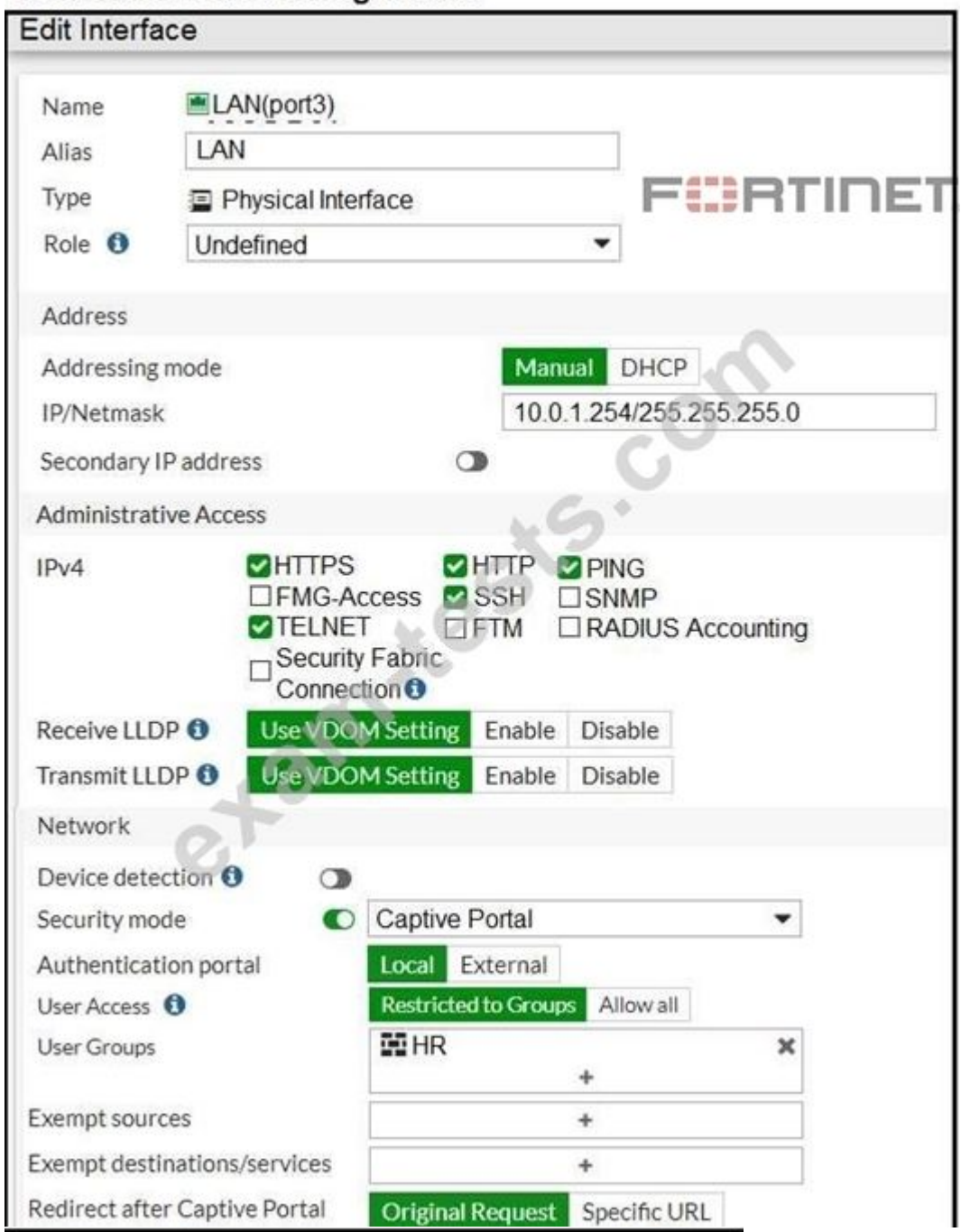
NEW QUESTION: 30

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: A,B,D (LEAVE A REPLY)
Explanation
Explanation/Reference:

NEW QUESTION: 31
Refer to the exhibit.
https://www.fast2test.com/NSE4_FGT-6.4-practice-test.html 17
Valid Fast2test NSE4_FGT-6.4 Exam PDF Dumps - New NSE4_FGT-6.4 Real Exam Questions

Network interface configuration



Enforce authentication on demand option enabled

```
Local-FortiGate # config user setting

Local-FortiGate (setting) # show
config user setting
     set auth-cert "Fortinet_Factory"
     set auth-on-demand always
end
```

Firewall policies

Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port3) → WAN(port1) 2						
Sales Users	Sales LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled
Auth-Users	LOCAL_SUBNET	all	always	ALL	ACCEPT	Enabled

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. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.

C. If there is a full-through policy in place, users will not be prompted for authentication.

D. Authentication is enforced at a policy level; all users will be prompted for authentication.

Answer: C (LEAVE A REPLY)

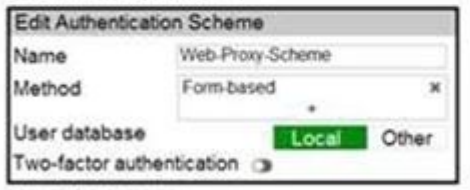
NEW QUESTION: 32

Refer to the exhibit.

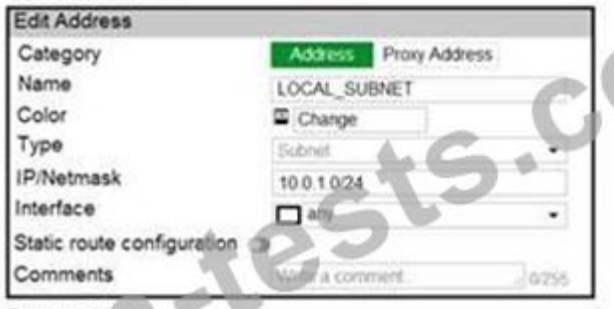
Authentication rule

Users

Authentication scheme



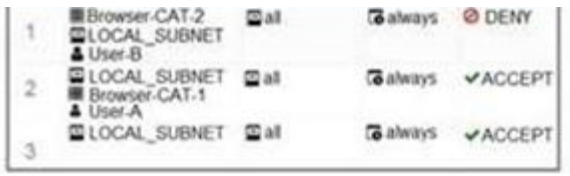
Firewall address



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 10.0.1.10 to the destination http://www.fortinet.com? (Choose two.)

A. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.

B. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

C. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.

D. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 33

Which statement about the policy ID number of a firewall policy is true?
D18912E1457D5D1DDCBD40AB3BF70D5D

A. It represents the number of objects used in the firewall policy.

B. It is required to modify a firewall policy using the CLI.

C. It defines the order in which rules are processed.

D. It changes when firewall policies are reordered.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 34

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. CLI diagnostics commands permission

C. Read/Write permission for Log & Report

D. Read/Write permission for Firewall

Answer: A (LEAVE A REPLY)

NEW QUESTION: 35

Examine the following web filtering log.

```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

Which statement about the log message is true?

A. The web site miniclip.com matches a static URL filter whose action is set to Warning.

B. The usage quota for the IP address 10.0.1.10 has expired

C. The name of the applied web filter profile is default.

D. The action for the category Games is set to block.

Answer: (SHOW ANSWER)

NEW QUESTION: 36

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 192.160.1.0/24 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. 192.168.0.0/24

B. 192.168.3.0/24

C. 192.168.2.0/24

D. 192.168.1.0/24

Answer: A (LEAVE A REPLY)

NEW QUESTION: 37

Refer to the exhibit.

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

A. Destination NAT is disabled in the firewall policy.

B. One-to-one NAT IP pool is used in the firewall policy.

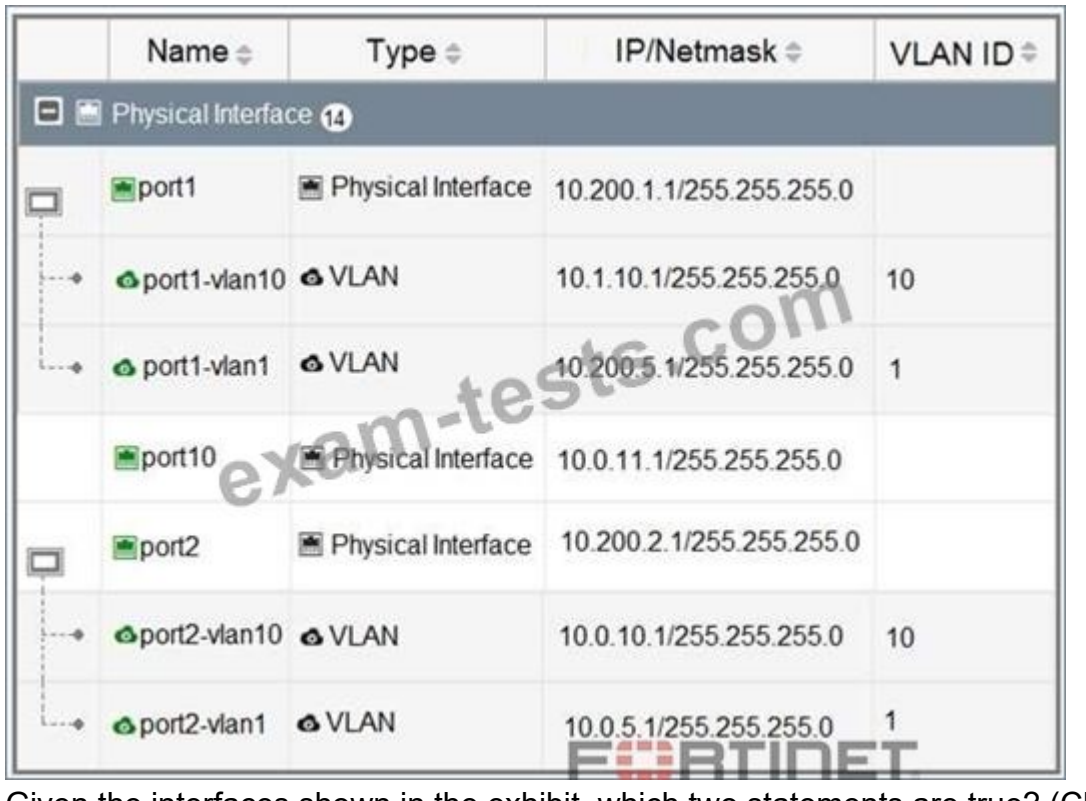
C. Port block allocation IP pool is used in the firewall policy.

D. Overload NAT IP pool is used in the firewall policy.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 38

Refer to the exhibit.



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

A. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

B. port1 is a native VLAN.

C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

D. Traffic between port2 and port2-vlan1 is allowed by default.

Answer: (SHOW ANSWER)

NEW QUESTION: 39

Which of the following SD-WAN load -balancing method use interface weight value to distribute traffic? (Choose two.)

A. Session

B. Volume

C. Source IP

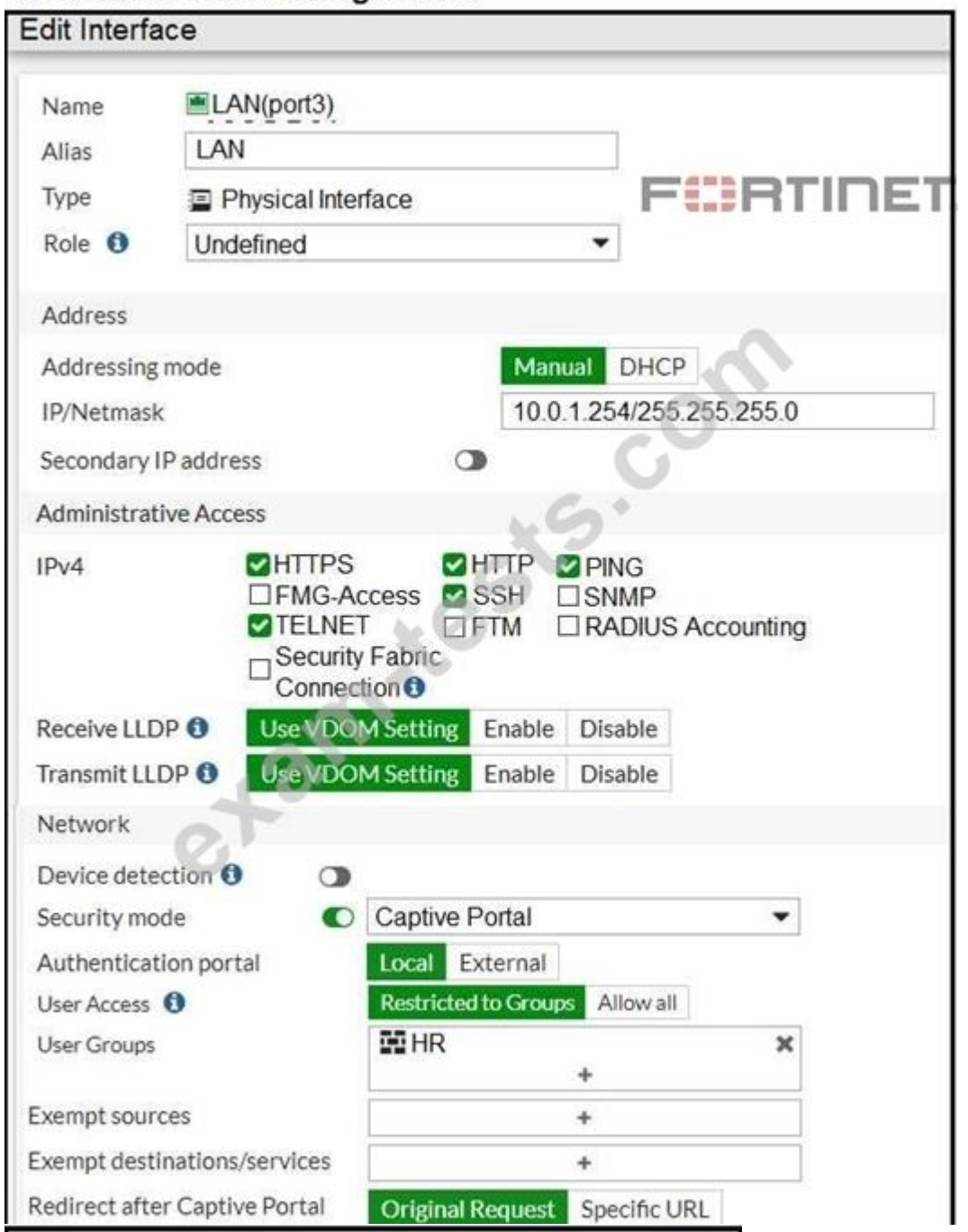
D. Spillover

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 40

Refer to the exhibit.

Network interface configuration



Enforce authentication on demand option enabled

```
Local-FortiGate # config user setting

Local-FortiGate (setting) # show
config user setting
     set auth-cert "Fortinet_Factory"
     set auth-on-demand always
end
```

Firewall policies

Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port3) → WAN(port1) 2						
Sales Users	Sales LOCAL_SUBNET	all	always	ALL	✔ ACCEPT	Enabled
Auth-Users	LOCAL_SUBNET	all	always	ALL	✔ ACCEPT	Enabled

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. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

B. Authentication is enforced at a policy level; all users will be prompted for authentication.

C. If there is a full-through policy in place, users will not be prompted for authentication.

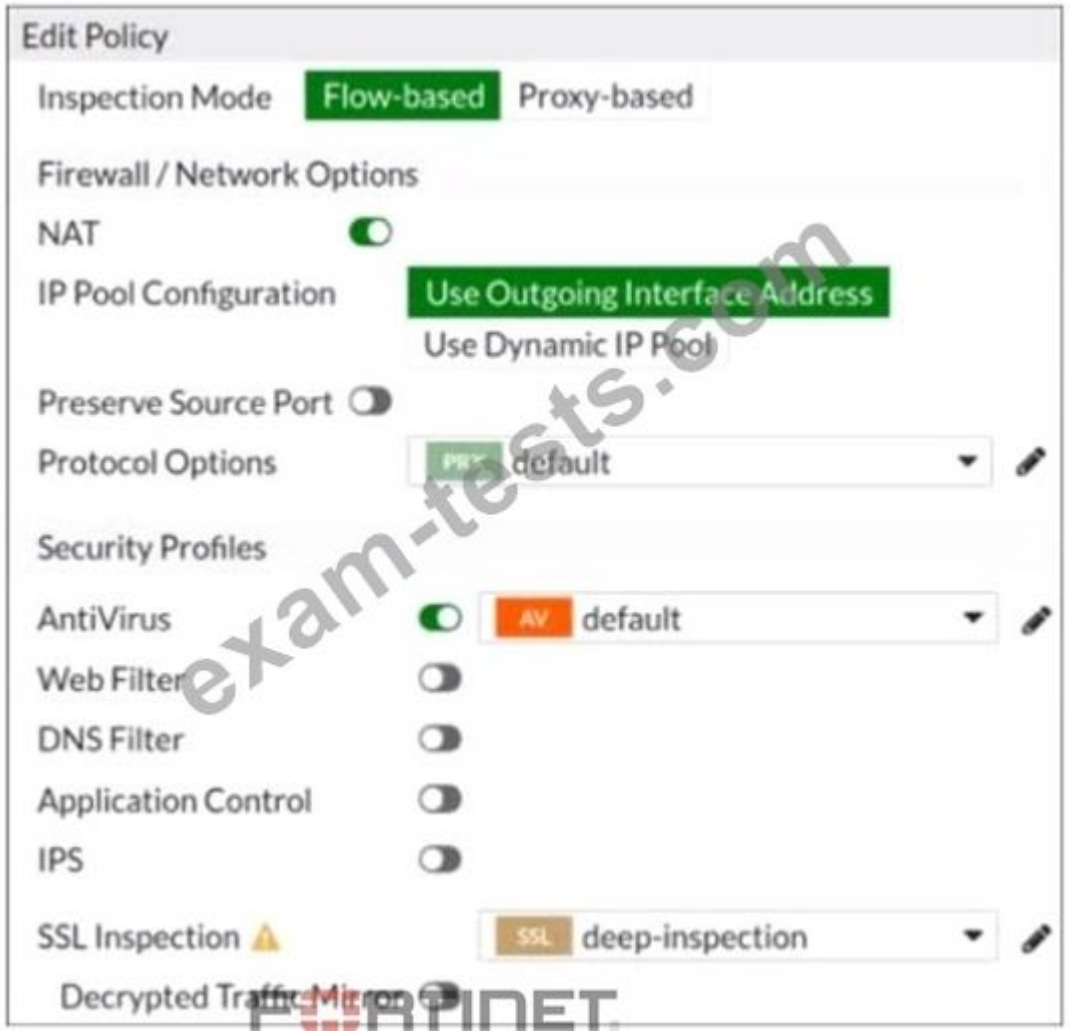
D. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.

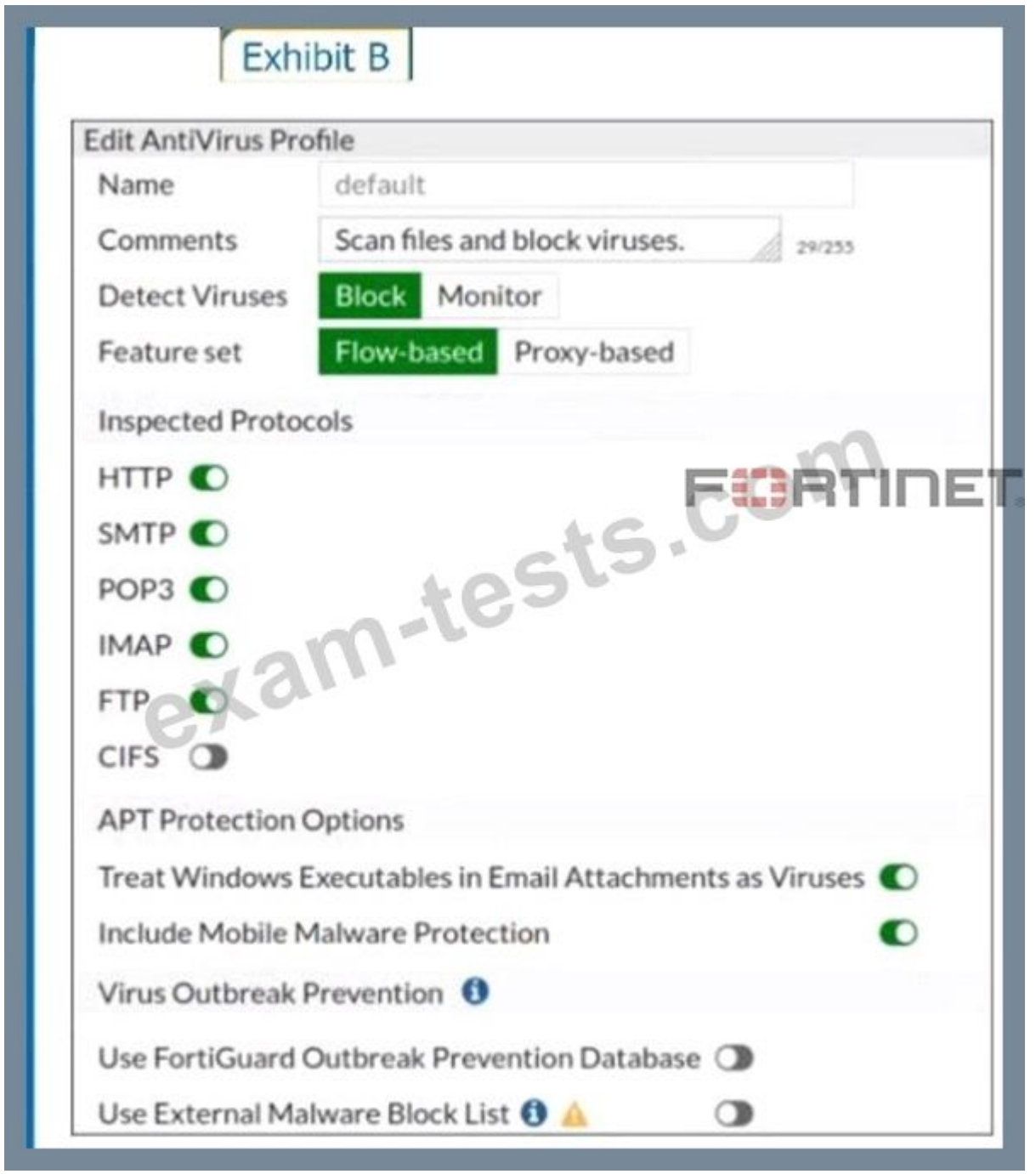
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41

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

Exhibit A





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 intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

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 firewall policy performs the full content inspection on the file.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 42

Examine the following web filtering log.

```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked reqtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

Which statement about the log message is true?

A. The name of the applied web filter profile is default.
B. The web site miniclip.com matches a static URL filter whose action is set to Warning.
C. The usage quota for the IP address 10.0.1.10 has expired
D. The action for the category Games is set to block.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
Refer to the exhibit to view the firewall policy.

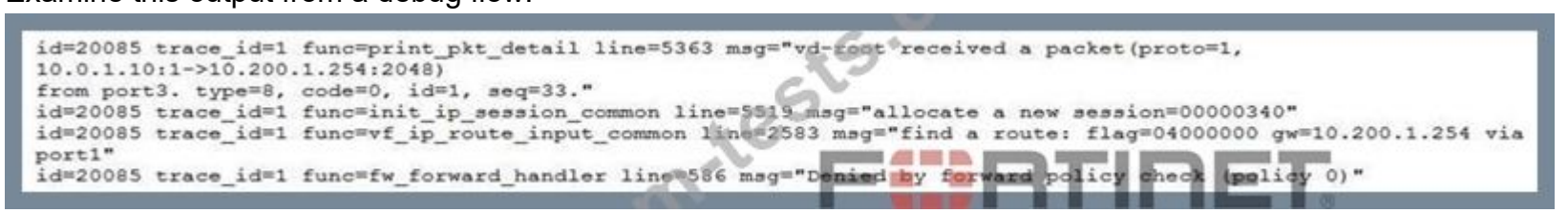
Which statement is correct if well-known viruses are not being blocked?

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

NEW QUESTION: 44
View the exhibit.

A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting Games). Based on this configuration, which statement is true?
A. Addcting.Games is allowed based on the Categories configuration.
B. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
C. Addicting.Games is allowed based on the Application Overrides configuration.
D. Addicting.Games is blocked on the Filter Overrides configuration.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
Examine this output from a debug flow:



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.

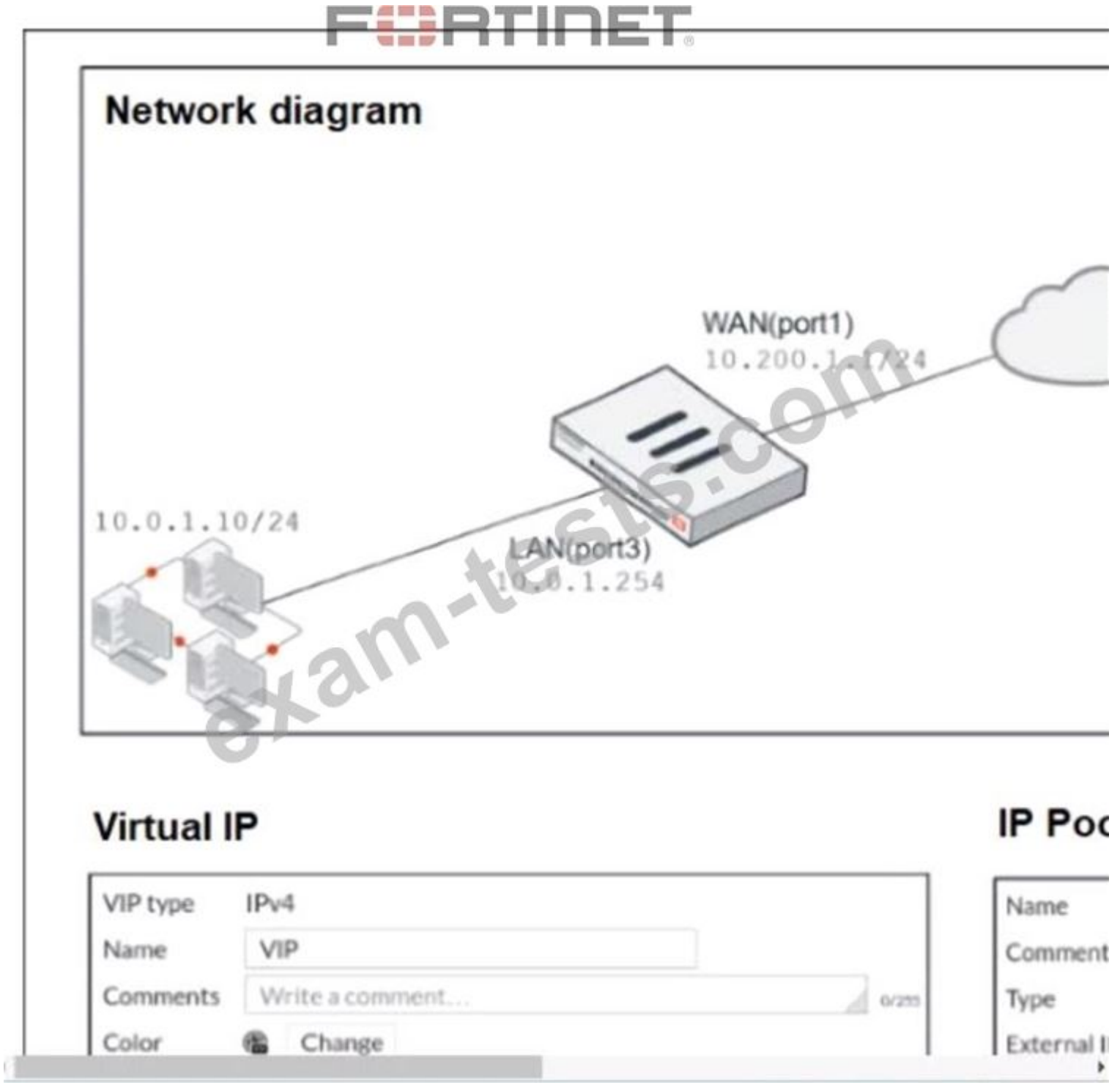
Answer: D (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 46

Refer to the exhibit.



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

The WAN (port1) interface has the IP address 10.200.1.1/24.

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

The first firewall policy has NAT enabled using IP Pool.
The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?
A. 10.200.1.1
B. 10.200.3.1
C. 10.200.1.100
D. 10.200.1.10
Answer: (SHOW ANSWER)

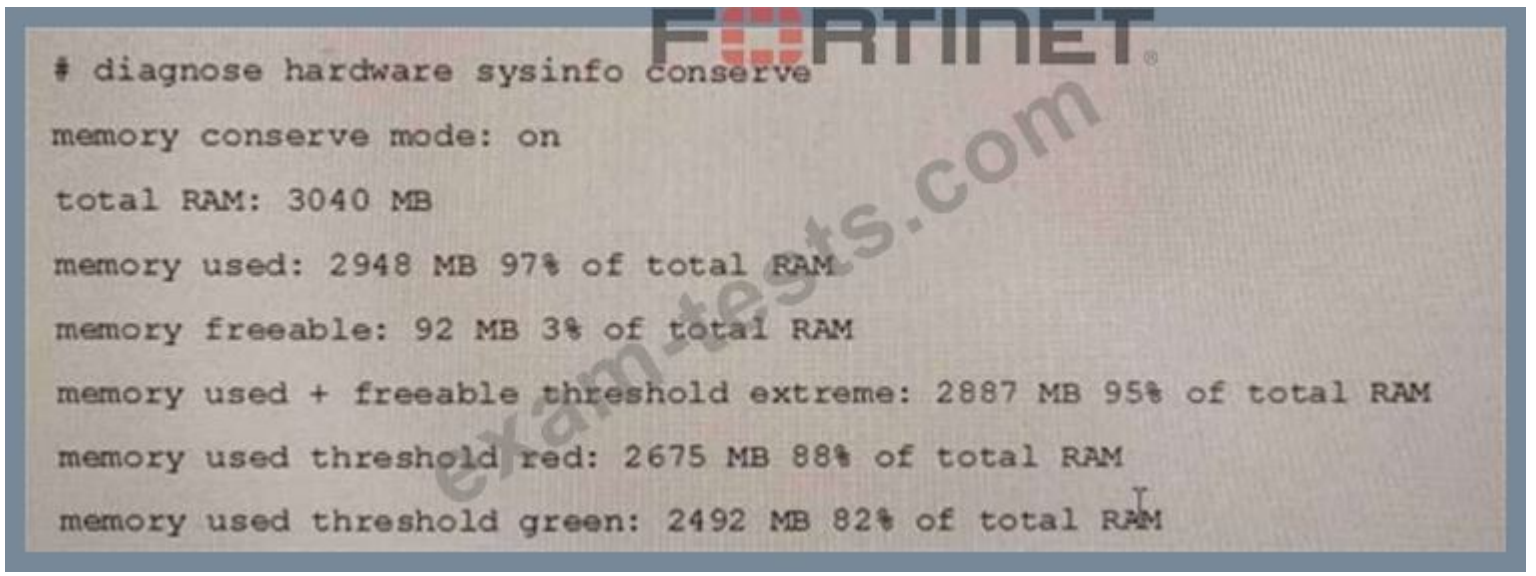
NEW QUESTION: 47
What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?
A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
B. FortiGate automatically negotiates a new security association after the existing security 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 (LEAVE A REPLY)
https://kb.fortinet.com/kb/documentLink.do?externalID=12069

NEW QUESTION: 48
Which two statements are true about collector agent advanced mode? (Choose two.)
A. Security profiles can be applied only to user groups, not individual users.
B. Advanced mode uses Windows convention-NetBios: Domain\Username.
C. Advanced mode supports nested or inherited groups
D. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 49
Examine this FortiGate configuration:

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

Examine the output of the following debug command:



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

A. It is allowed and inspected as long as the inspection is flow based

B. It is dropped.

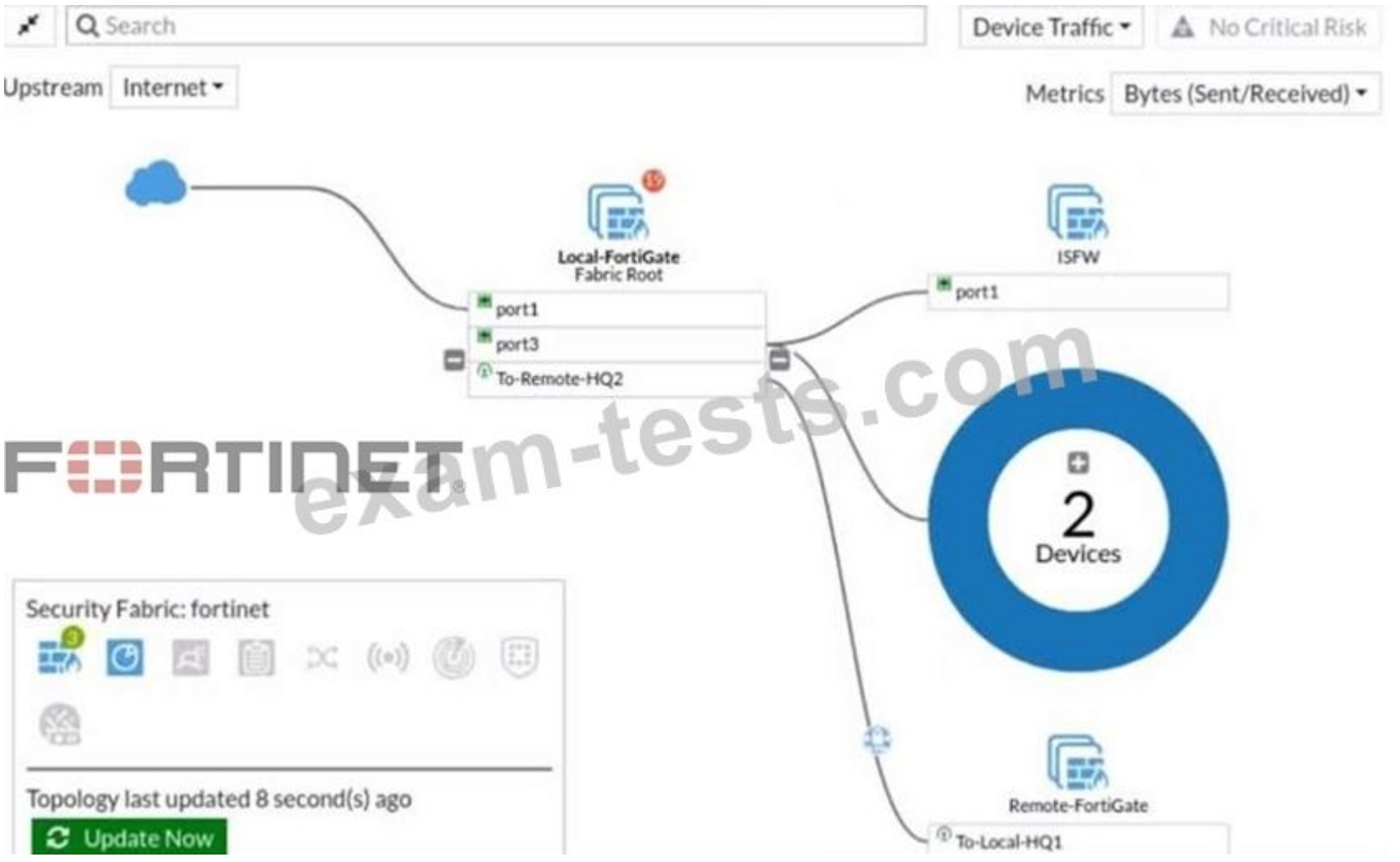
C. It is allowed and inspected, as long as the only inspection required is antivirus.

D. It is allowed, but with no inspection

Answer: B (LEAVE A REPLY)

NEW QUESTION: 50

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.

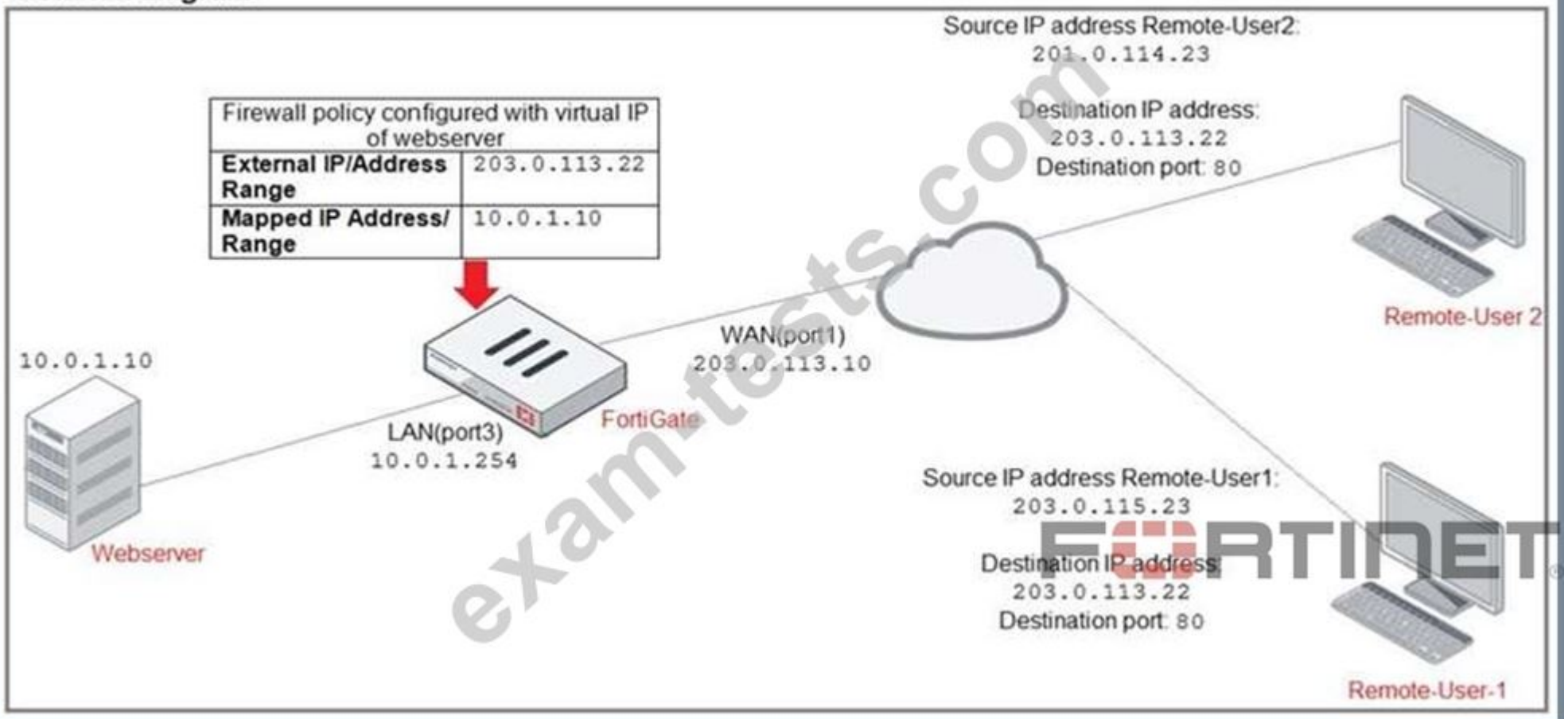
D. Device detection is disabled on all FortiGate devices.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 51

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. Enable match vip in the Deny policy.

B. Disable match-vip in the Deny policy.

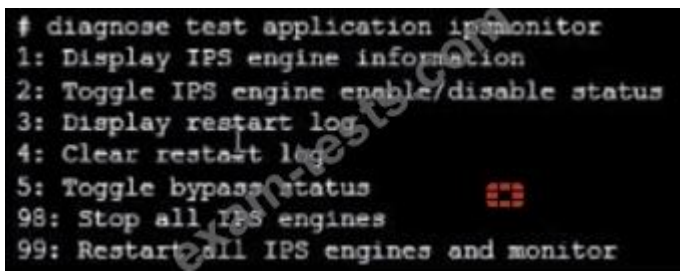
C. Set the Destination address as Deny_IP in the Allow-access policy.

D. Set the Destination address as Web_server in the Deny policy.

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 52

Refer to the exhibit.



Examine the intrusion prevention system (IPS) diagnostic command.

Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.

B. The IPS engine was blocking all traffic.

C. The IPS engine was unable to prevent an intrusion attack.

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 53
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. Intrusion prevention
D. DNS filter
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 54
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 must use the user self-registration server.
B. The administrator must use a FortiAuthenticator device.
C. The administrator can register the same FortiToken on more than one FortiGate.
D. The administrator can use a third-party radius OTP server.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 55
View the exhibit.

Which of the following statements are correct? (Choose two.)
A. This is a redundant IPsec setup.
B. This setup requires at least two firewall policies with the action set to IPsec.
C. Dead peer detection must be disabled to support this type of IPsec setup.
D. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.
Answer: (SHOW ANSWER)

NEW QUESTION: 56
View the exhibit. A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting Games). Based on this

A. Addcting.Games is allowed based on the Categories configuration.

B. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.

C. Addicting.Games is blocked on the Filter Overrides configuration.

D. Addicting.Games is allowed based on the Application Overrides configuration.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 57

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
```

A. Denied users are blocked for 30 minutes.

B. The number of logs generated by denied traffic is reduced.

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

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

C. Device detection on all interfaces is enforced for 30 minutes.

D. A session for denied traffic is created.

Answer: (SHOW ANSWER)

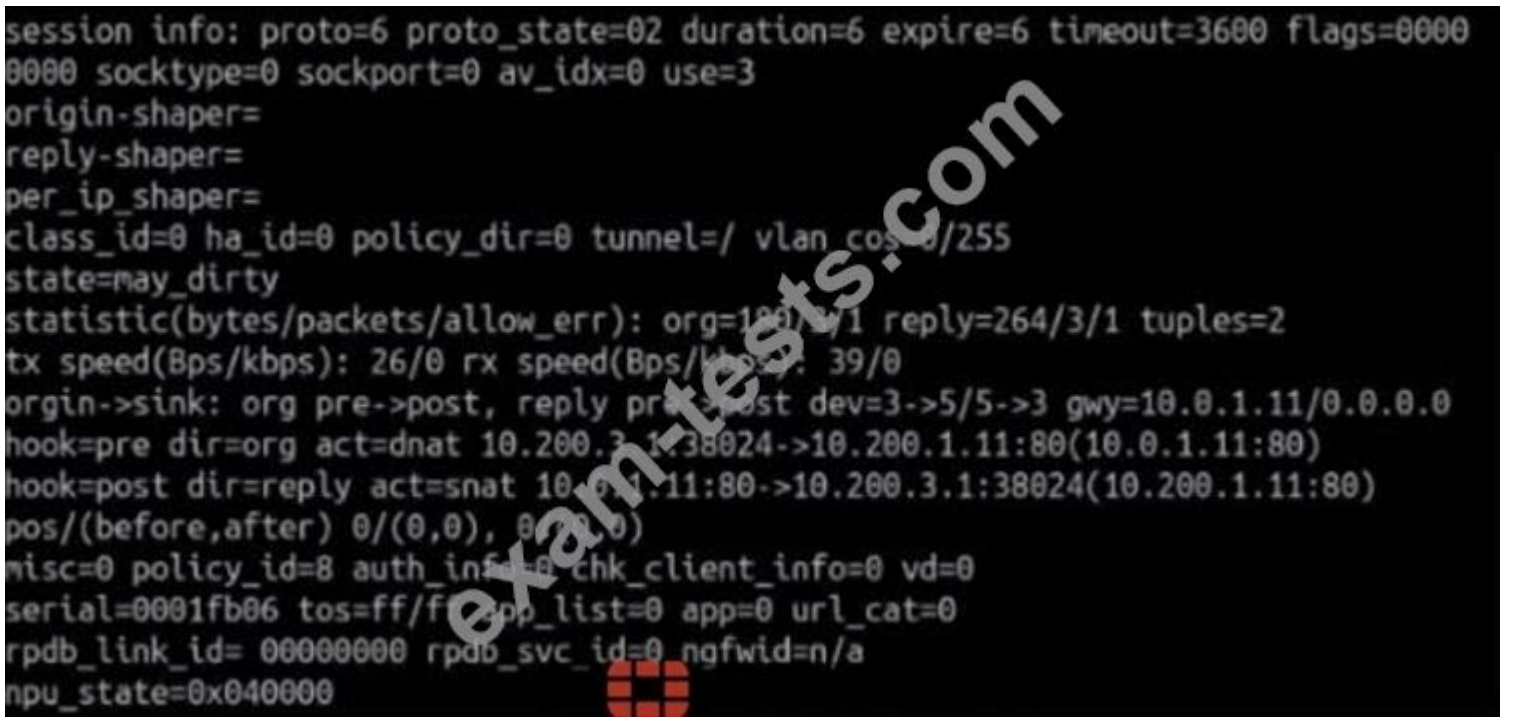
NEW QUESTION: 58

In an explicit proxy setup, where is the authentication method and database configured?

A. Firewall Policy

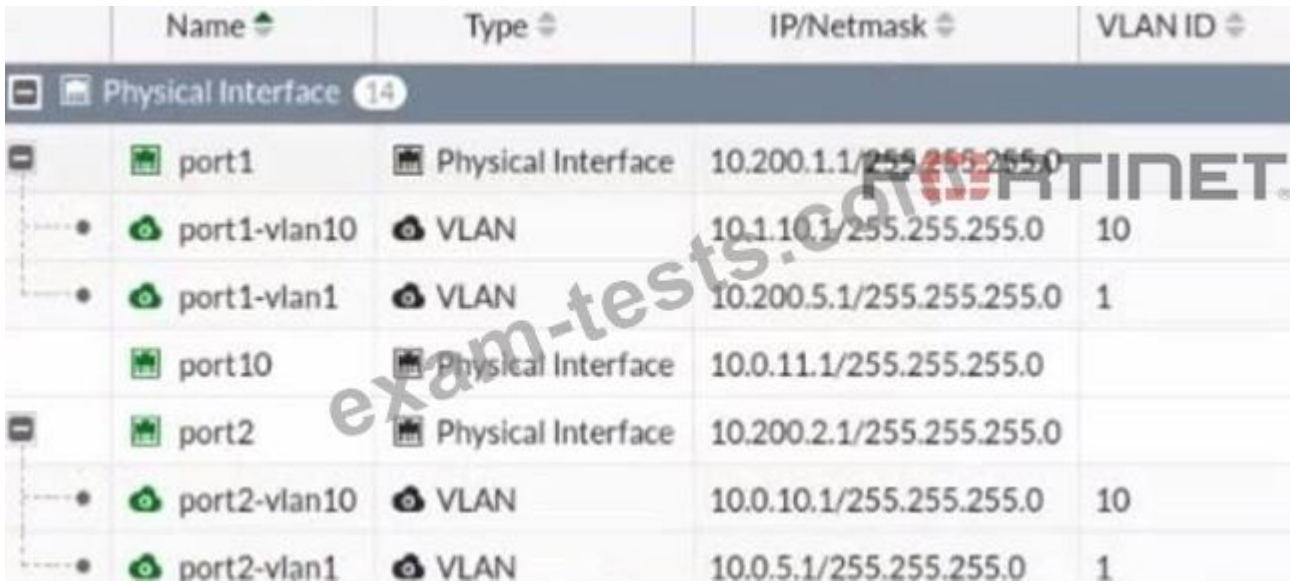
B. Authentication Rule
C. Authentication scheme
D. Proxy Policy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
Refer to the exhibit.



Which contains a session diagnostic output. Which statement is true about the session diagnostic output?
A. The session is in SYN_SENT state.
B. The session is in FIN_ACK state.
C. The session is in FTN_WAIT state.
D. The session is in ESTABLISHED state.
Answer: (SHOW ANSWER)
Indicates TCP (proto=6) session in SYN_SENT state (proto=state=2) https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042

NEW QUESTION: 60
Refer to the exhibit.



Name	Type	IP/Netmask	VLAN ID
Physical Interface 14			
port1	Physical Interface	10.200.1.1/255.255.255.0	
port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
port10	Physical Interface	10.0.11.1/255.255.255.0	
port2	Physical Interface	10.200.2.1/255.255.255.0	
port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

A. port1 is a native VLAN.

B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

C. Traffic between port2 and port2-vlan1 is allowed by default.

D. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs

Answer: (SHOW ANSWER)

NEW QUESTION: 61

Refer to the exhibit.

```
STUDENT # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT          DESTINATION        DESTINATION-NAT
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?

A. One-to-one NAT IP pool is used in the firewall policy.

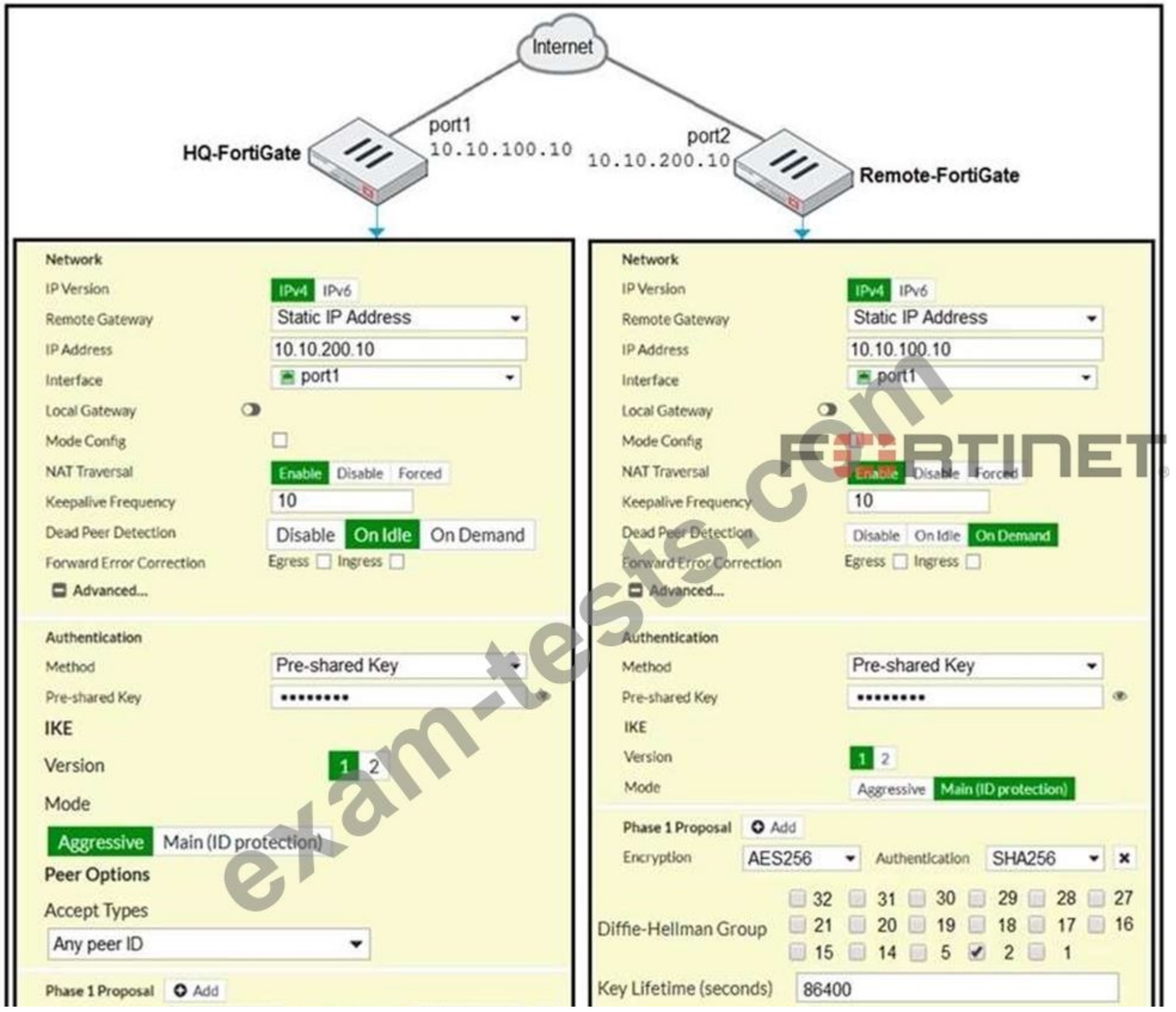
B. Overload NAT IP pool is used in the firewall policy.

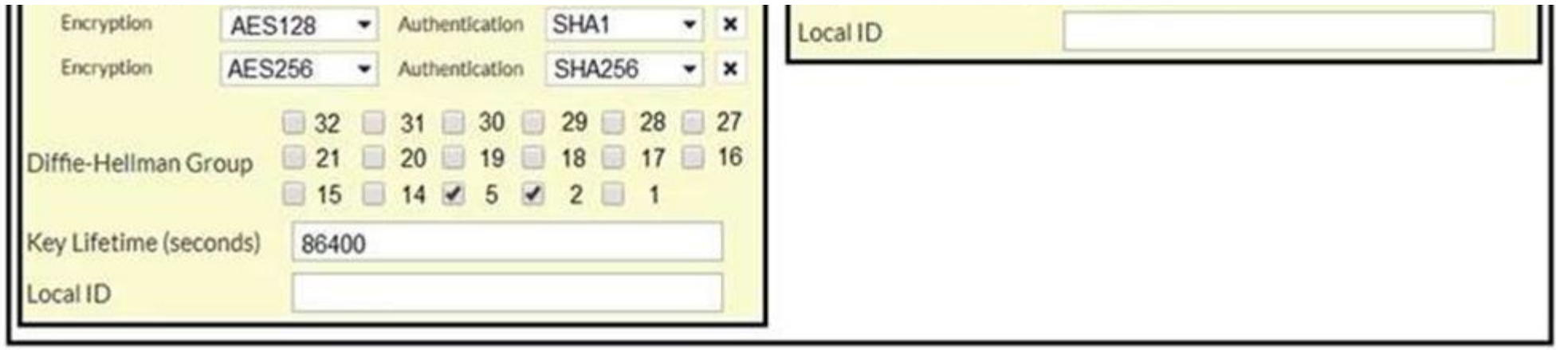
C. Port block allocation IP pool is used in the firewall policy.

D. Destination NAT is disabled in the firewall policy.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 62
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, disable Diffie-Helman group 2.

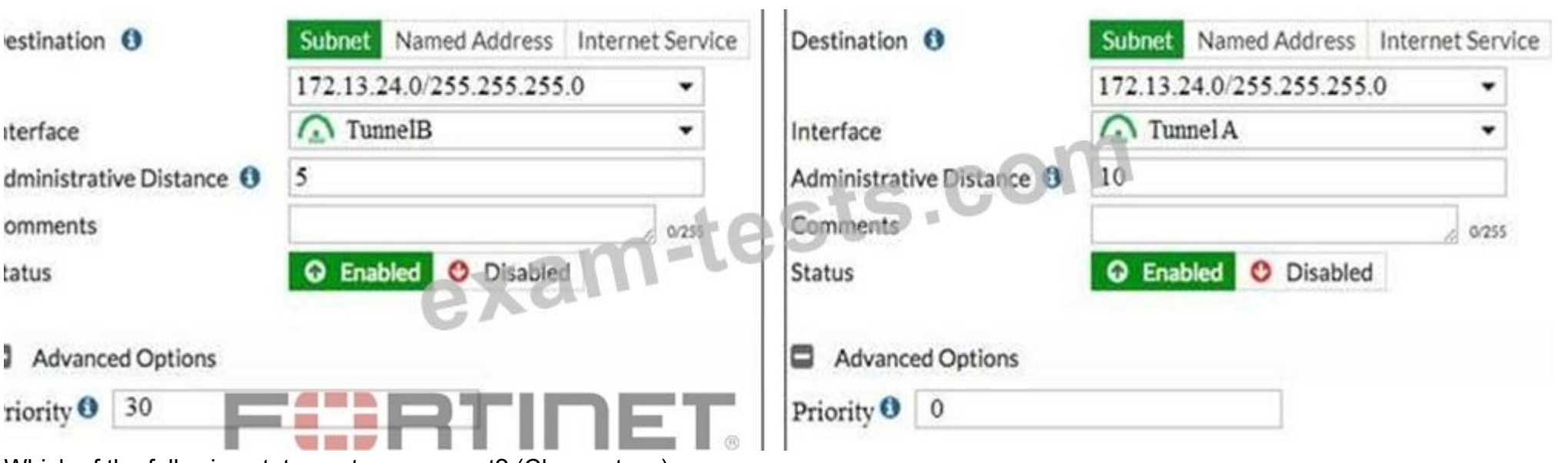
B. On HQ-FortiGate, set IKE mode to Main (ID protection).

C. On Remote-FortiGate, set port2 as Interface.

D. On both FortiGate devices, set Dead Peer Detection to On Demand.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 63
View the exhibit.



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

A. Dead peer detection must be disabled to support this type of IPsec setup.

B. This is a redundant IPsec setup.

C. The TunnelB route is the primary route for reaching the remote site. The TunnelA route is used only if the TunnelB VPN is down.

D. This setup requires at least two firewall policies with the action set to IPsec.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 64

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. The collector agent must search security event logs.

C. The NetSession Enum function is used to track user logouts.

D. NetAPI polling can increase bandwidth usage in large networks.

Answer: (SHOW ANSWER)

NEW QUESTION: 65

Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Flow engine

B. Detection engine

C. Intrusion prevention system engine

D. Antivirus engine

Answer: C (LEAVE A REPLY)

NEW QUESTION: 66

If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source filed of a firewall policy?

A. User or User Group

B. Once Internet Service is selected, no other object can be added

C. FQDN address

D. IP address

Answer: D (LEAVE A REPLY)

NEW QUESTION: 67

Refer to the exhibit.

```
FGT1 # get router info routing-table database
Codes:  K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        > -  selected route, * - FIB route, p - stale info

S       *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
        *>                  [10/0] via 10.0.0.2, port2, [30/0]
S          0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C       *> 10.0.0.0/24 is directly connected, port2
S          172.13.24.0/24  [10.0] is directly connected, port4
C       *> 172.20.121.0/24 is directly connected, port1
S       *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C       *> 192.168.15.0/24 is directly connected, port3
```

Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)

A. There will be eight routes active in the routing table.

B. The port3 default route has the lowest metric.

C. The port3 default route has the highest distance.

D. The port1 and port2 default routes are active in the routing table.

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 68

Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

A. Lookup is done on the trust reply packet from the re spender

B. Lookup is done on the trust packet from the session originator

C. Lookup is done on every packet, regardless of direction

D. Lookup is done on the last packet sent from the re spender

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 69

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. A session for denied traffic is created.

B. The number of logs generated by denied traffic is reduced.

C. Device detection on all interfaces is enforced for 30 minutes.

D. Denied users are blocked for 30 minutes.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 70

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. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.

C. port-VLAN1 is the native VLAN for the port1 physical interface.

D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 71
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. Is used to discover FortiGate devices in different HA groups
D. Runs only over the heartbeat links
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 72
Refer to the exhibit, which contains a static route configuration.

An administrator created a static route for Amazon Web Services.
What CLI command must the administrator use to view the route?
A. get router info routing-table database
B. diagnose firewall proute list
C. get internet service route list
D. get router info routing-table all
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
Refer to the exhibits.

SSL-VPN Settings

FORTINET

Connection Settings

Listen on Interface(s) port1

Listen on Port 10443

Web mode access will be listening at https://10.200.1.1:10443

Redirect HTTP to SSL-VPN

Restrict Access Allow access from any host | Limit access to specific hosts

Idle Logout

Inactive For 300 Seconds

Server Certificate Fortinet_Factory

Require Client Certificate

Tunnel Mode Client Settings

Address Range Automatically assign addresses | Specify custom IP ranges

Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server Same as client system DNS | Specify

Specify WINS Servers

Authentication/Portal Mapping

+ Create New | Edit | Delete

Users/Groups	Portal
sslvpn	tunnel-access
All Other Users/Groups	full-access

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 portal to the tunnel.

B. Change the idle-timeout.

C. Change the Server IP address.

D. Change the SSL VPN port on the client.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

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. Access to the social networking web filter category was explicitly blocked to all users.

B. The action on firewall policy ID 1 is set to warning.

C. Social networking web filter category is configured with the action set to authenticate.

D. The name of the firewall policy is all_users_web.

Answer: (SHOW ANSWER)

NEW QUESTION: 75

An administrator is configuring an IPsec VPN between site A and site B.

The Remote Gateway setting in both sites has been configured as. 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. 192.168.3.0/24

C. 192.168.2.0/24

D. 192.168.0.0/24

Answer: C (LEAVE A REPLY)

NEW QUESTION: 76

In a high availability (HA) cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?

A. Client > primary FortiGate> secondary FortiGate> primary FortiGate> web server.

B. Client > secondary FortiGate> web server.

C. Client >secondary FortiGate> primary FortiGate> web server.

D. Client> primary FortiGate> secondary FortiGate> web server.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 77

Refer to the exhibit.

Network interface configuration

Edit Interface

Name: LAN(port3)

Alias: LAN

Type: Physical Interface

Role: Undefined

Address

Addressing mode: Manual | DHCP

IP/Netmask: 10.0.1.254/255.255.255.0

Secondary IP address: ○

Administrative Access

IPv4:
- ☑ HTTPS
- ☑ HTTP
- ☑ PING
- ☐ FMG-Access
- ☑ SSH
- ☐ SNMP
- ☑ TELNET
- ☐ FTM
- ☐ RADIUS Accounting
- ☐ Security Fabric Connection

Receive LLDP: Use VDOM Setting | Enable | Disable

Transmit LLDP: Use VDOM Setting | Enable | Disable

Network

Device detection: ○

Security mode: ● Captive Portal

Authentication portal: Local | External

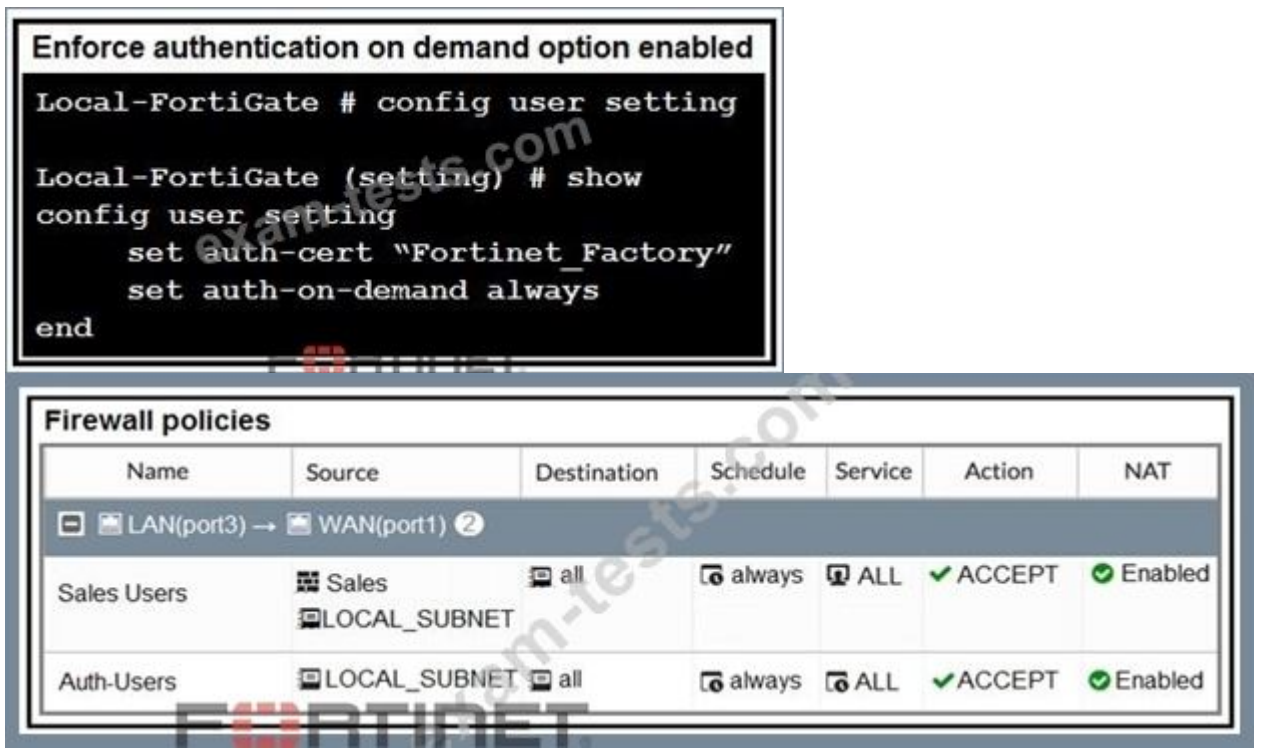
User Access: Restricted to Groups | Allow all

User Groups: HR

Exempt sources: +

Exempt destinations/services: +

Redirect after Captive Portal: Original Request | Specific URL



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. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

B. Authentication is enforced at a policy level; all users will be prompted for authentication.

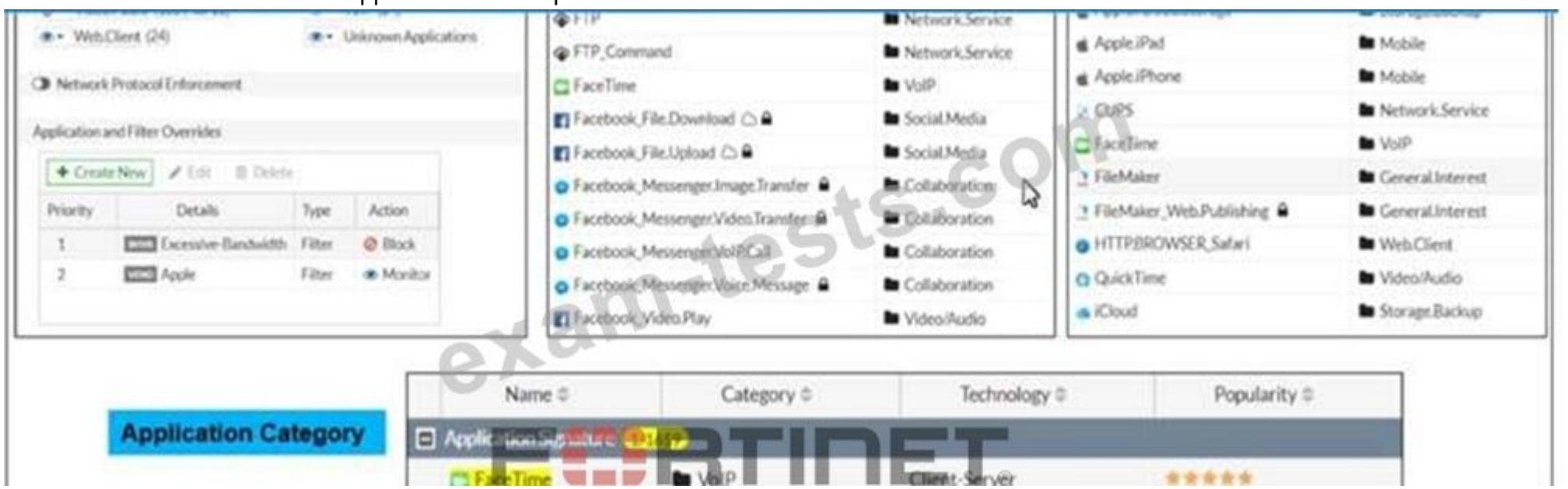
C. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.

D. If there is a full-through policy in place, users will not be prompted for authentication.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 78

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 allowed, based on the Apple filter configuration.

B. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn

C. Apple FaceTime will be allowed, based on the Categories configuration.
D. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
Answer: D (LEAVE A REPLY)

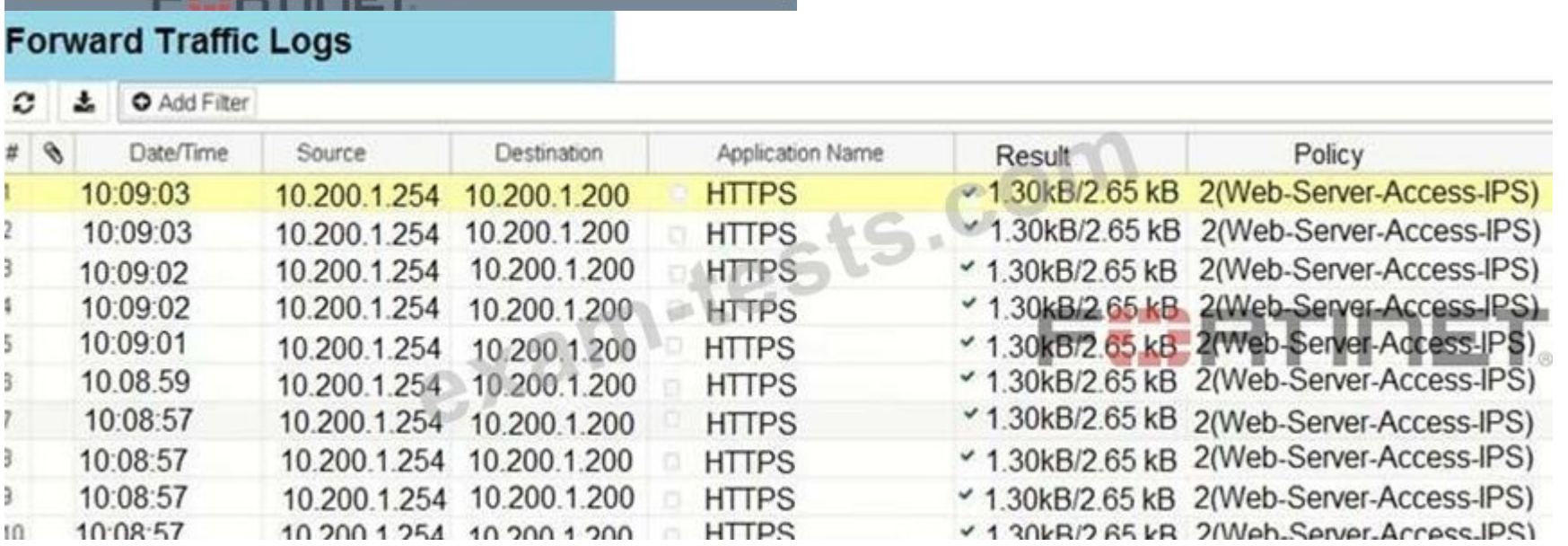
NEW QUESTION: 79
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?
A. It limits the scope of application control to the browser-based technology category only.
B. It limits the scope of application control to scan application traffic using parent signatures only
C. It limits the scope of application control to scan application traffic based on application category only.
D. It limits the scope of application control to scan application traffic on DNS protocol only.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 80
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 generate logs
B. To remove the NAT operation.
C. To allow for out-of-order packets that could arrive after the FIN/ACK packets.
D. To finish any inspection operations.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 81
Refer to the exhibit, which contains a static route configuration.

An administrator created a static route for Amazon Web Services.
What CLI command must the administrator use to view the route?
A. get router info routing-table all
B. get router info routing-table database
C. get internet service route list
D. diagnose firewall proute list
Answer: D (LEAVE A REPLY)
NEW QUESTION: 82

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 firewall policy is not using a full SSL inspection profile.

B. The HTTPS signatures have not been added to the sensor.

C. The IPS filter is missing the Protocol: HTTPS option.

D. A DoS policy should be used, instead of an IPS sensor.

E. A DoS policy should be used, instead of an IPS sensor.

Answer: (SHOW ANSWER)

NEW QUESTION: 83

What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

A. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

B. FortiGate automatically negotiates a new security association after the existing security association expires.

C. FortiGate automatically negotiates different local and remote addresses with the remote peer.

D. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 84
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. Traffic matching the signature will be silently dropped and logged.
B. The signature setting uses a custom rating threshold.
C. The signature setting includes a group of other signatures.
D. Traffic matching the signature will be allowed and logged.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 85
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: (SHOW ANSWER)
Explanation
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

NEW QUESTION: 86
Examine this FortiGate configuration:

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 and inspected as long as the inspection is flow based

B. It is allowed, but with no inspection

C. It is dropped.

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 87

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 policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

C. The Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.

D. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.

E. The IP version of the sources and destinations in a policy must match.

Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 88

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. FortiGuaid update servers

B. NGFW mode

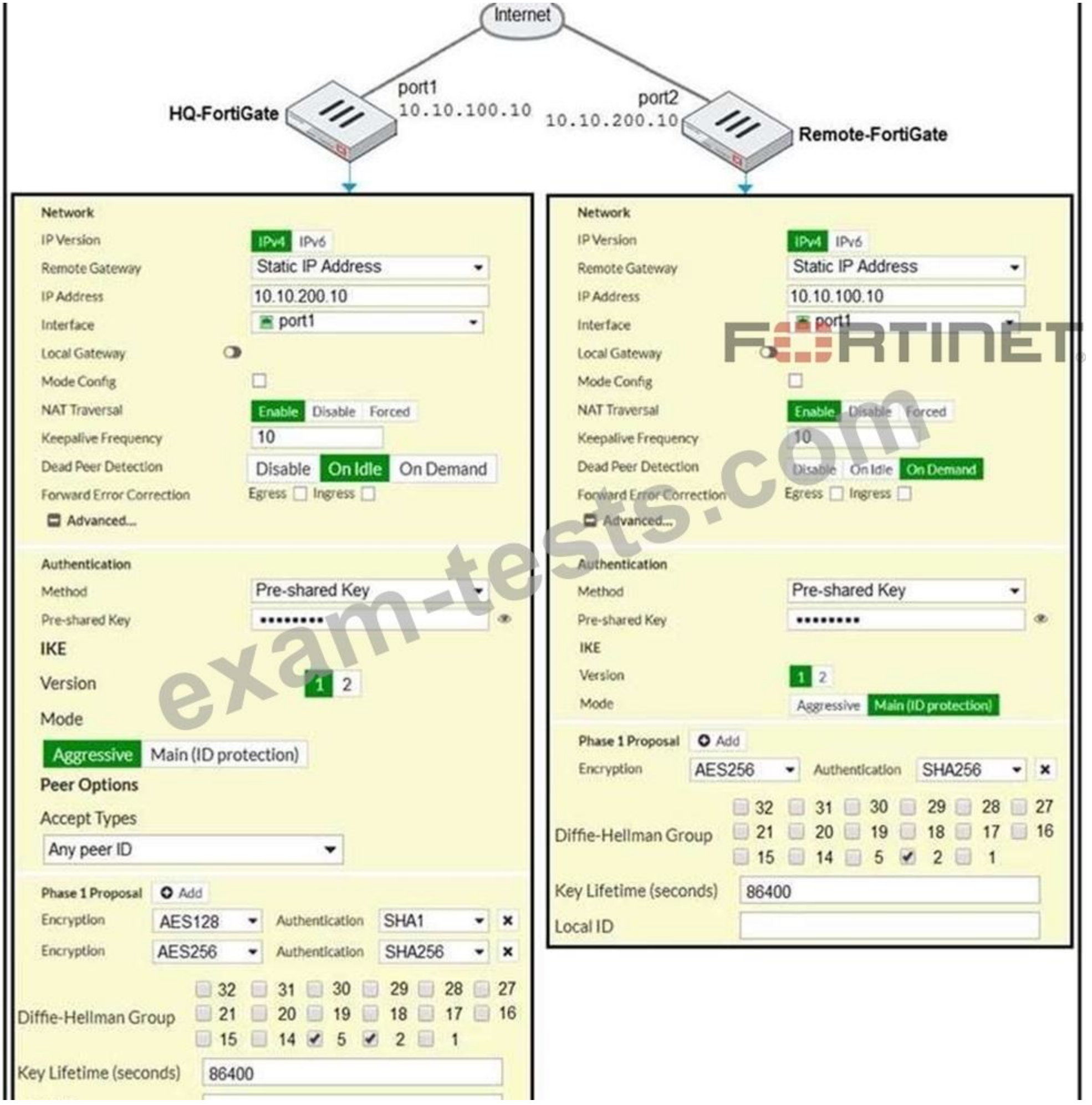
C. Operating mode

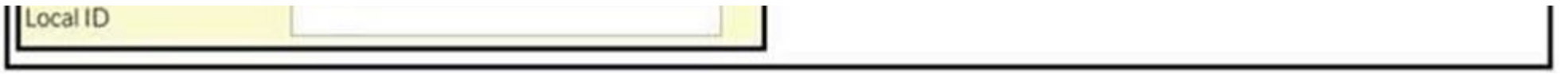
D. System time

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 89

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, disable Diffie-Helman group 2.

B. On Remote-FortiGate, set port2 as Interface.

C. On HQ-FortiGate, set IKE mode to Main (ID protection).

D. On both FortiGate devices, set Dead Peer Detection to On Demand.

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 90

Refer to the exhibit.

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

A. Custom permission for Network

B. Read/Write permission for Log & Report

C. CLI diagnostics commands permission

D. Read/Write permission for Firewall

Answer: C (LEAVE A REPLY)

Explanation

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

NEW QUESTION: 91
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)
A. FortiAnalyzer
B. FortiCache
C. FortiSandbox
D. FortiSIEM
E. FortiCloud
Answer: A,D,E (LEAVE A REPLY)

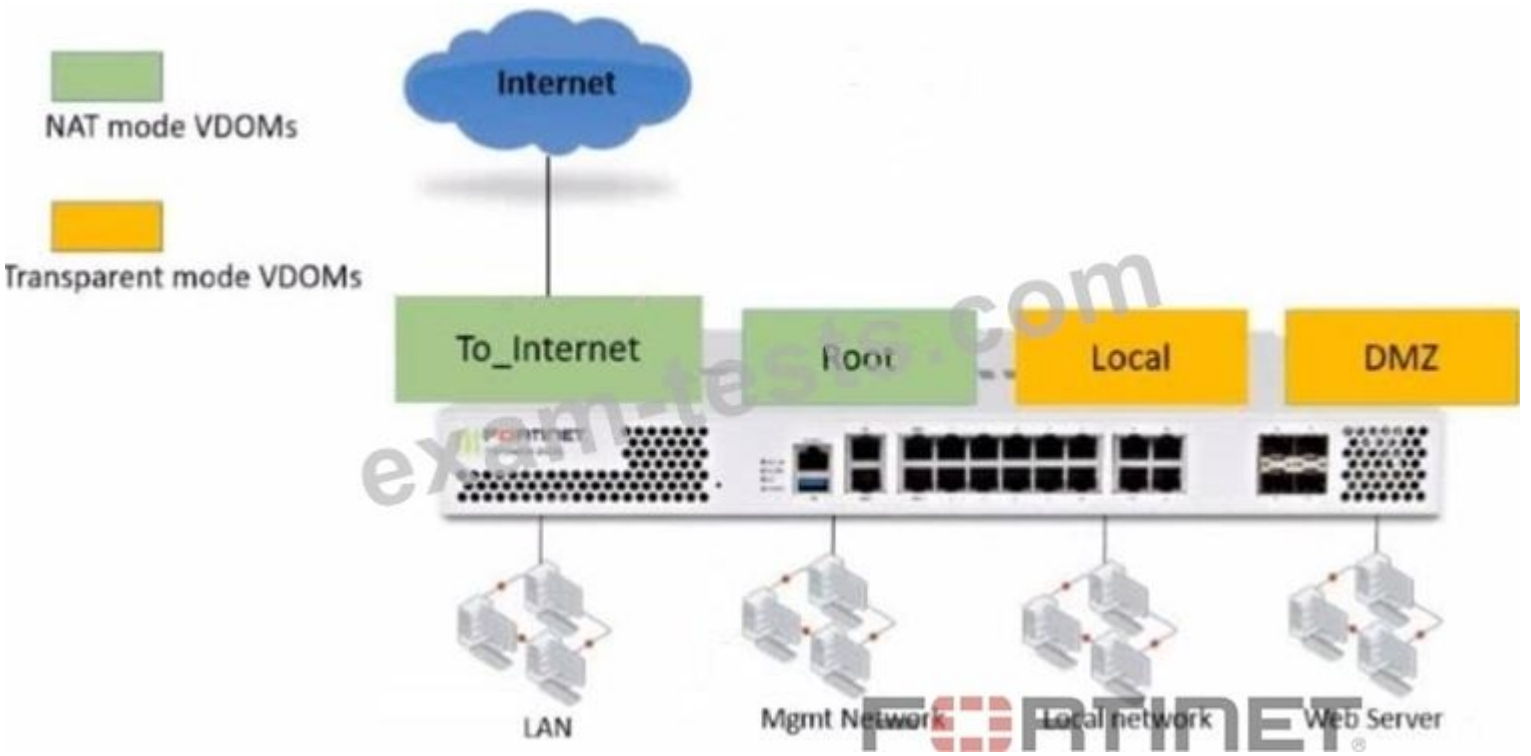
NEW QUESTION: 92
FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.
Which two other security profiles can you apply to the security policy? (Choose two.)
A. File filter
B. Intrusion prevention
C. Antivirus scanning
D. DNS filter
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 93
An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.2" 5
```

Which three pieces of Information will be Includedin me sniffer output? {Choose three.)
A. Interface name
B. Packetpayload
C. Application header
D. Ethernet header
E. IP header
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 94



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access internet.
The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
Which two statements are true? (Choose two.)

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.

B. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

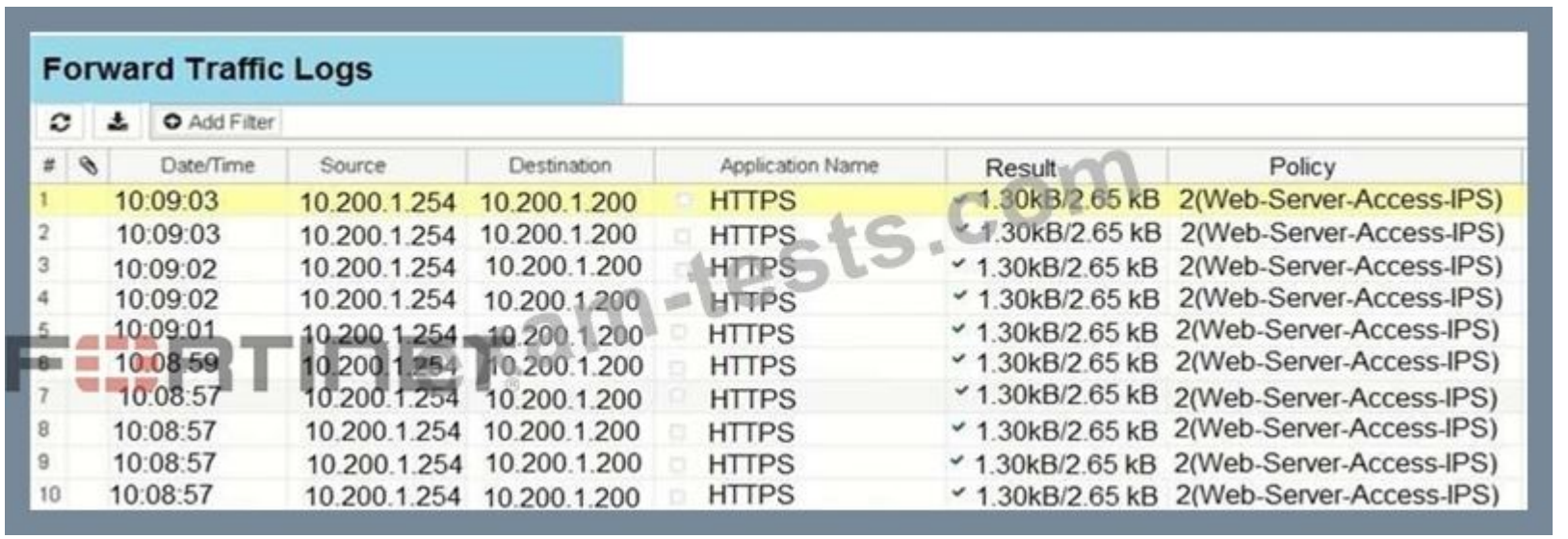
C. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.

D. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 95

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. A DoS policy should be used, instead of an IPS sensor.

C. A DoS policy should be used, instead of an IPS sensor.

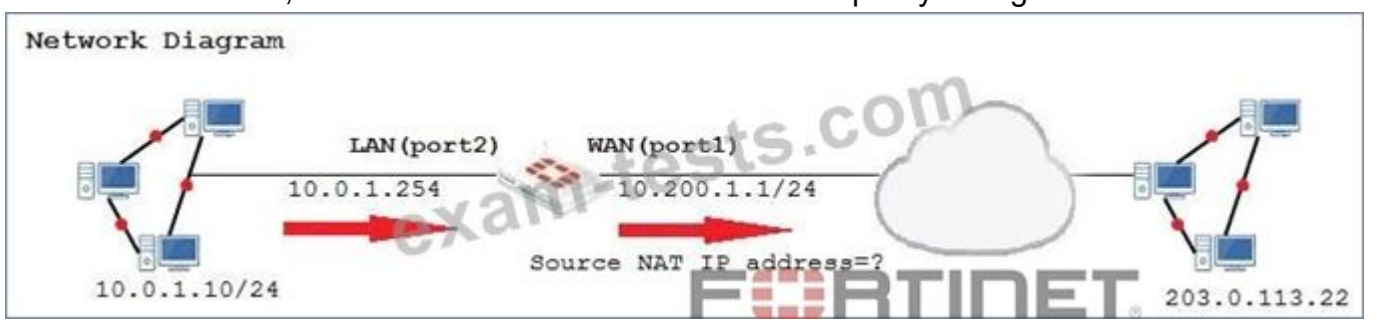
D. The firewall policy is not using a full SSL inspection profile.

E. The HTTPS signatures have not been added to the sensor.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 96

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 (LEAVE A REPLY)

Explanation

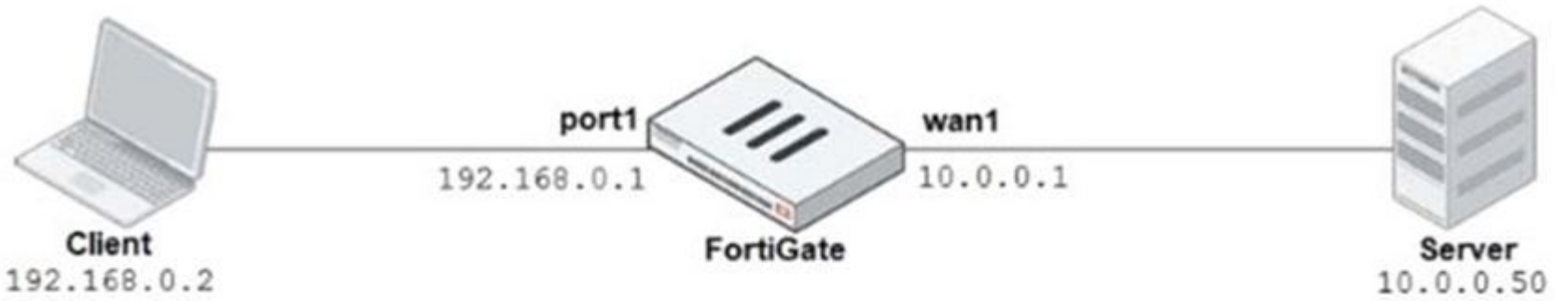
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs.

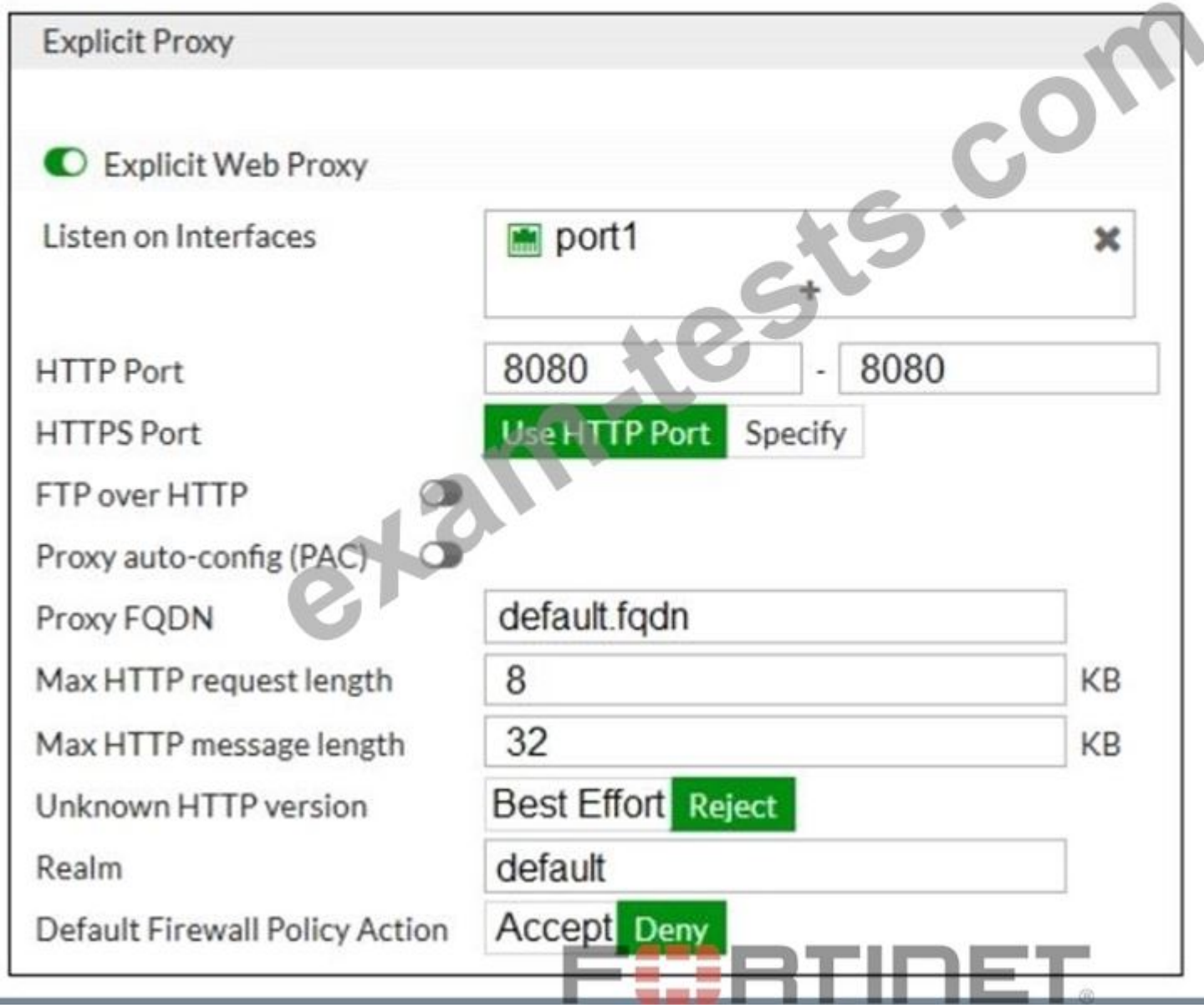
NEW QUESTION: 97

Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache
B. FortiAnalyzer
C. FortiSandbox
D. FortiSIEM
E. FortiCloud
Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 98
Refer to the exhibit.





The exhibits show a network diagram and the explicit web proxy configuration.

In the command diagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

A. 'host 192.168.0.1 and port 80'

B. 'host 10.0.0.50 and port 80'

C. 'host 10.0.0.50 and port 8080'

D. 'host 192.168.0.2 and port 8080'

Answer: (SHOW ANSWER)

NEW QUESTION: 99

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale     : english

Service    : Web-Filter
Status     : Enable
License    : Contract

Num. of servers     : 1
Protocol            : https
Port                : 443
Anycast             : Enable
Default servers     : Not included
-=- Server List (Tue Feb 1 12:00:25 2020) -=-

IP                   Weight        RTT  Flags     TZ        Packets   Curr Lost  Total Lost
173.243.138.210          10         85  DI        -8            868           0           0
96.45.33.68              10        270            -8            868           0           0
173.243.138.211          10        340            -8            859           0           0
```

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

A. There is at least one server that lost packets consecutively.

B. One server was contacted to retrieve the contract information.

C. FortiGate is using default FortiGuard communication settings.

D. A local FortiManager is one of the servers FortiGate communicates with.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 100

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=5760 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 port1. 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.)

A. The default route is required to receive a reply.

B. The debug flow is of ICMP traffic.

C. A firewall policy allowed the connection.

D. A new traffic session is created.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 101
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. Policy ID
C. Sequence ID
D. Universally Unique Identifier
Answer: D (LEAVE A REPLY)

NEW QUESTION: 102
Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)
A. Web application firewall
B. Antivirus in flow-based inspection
C. Web filter in flow-based inspection
D. DNS filter
E. Application control
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 103
Refer to the exhibit.

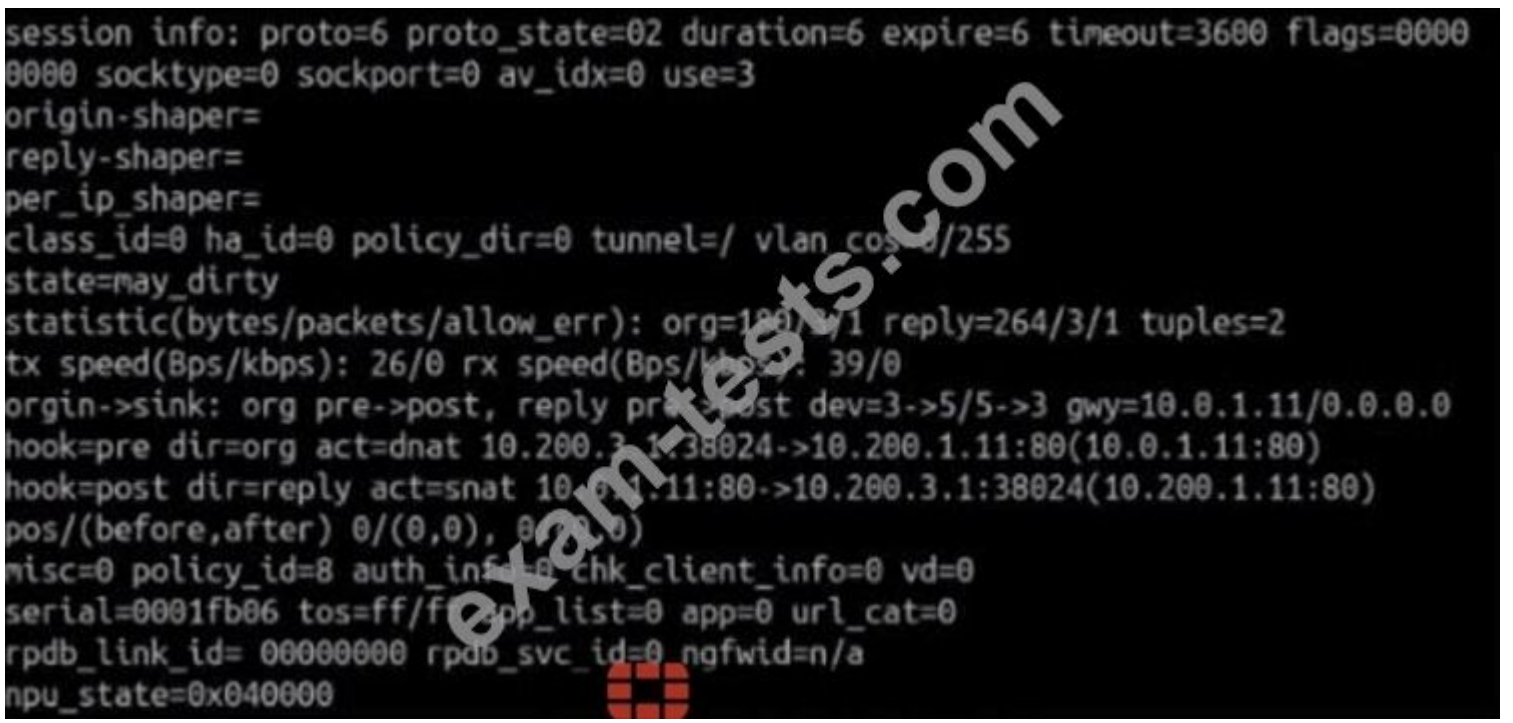
Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?
A. The signature setting uses a custom rating threshold.
B. The signature setting includes a group of other signatures.
C. Traffic matching the signature will be allowed and logged.
D. Traffic matching the signature will be silently dropped and logged.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)
A. System time
B. Operating mode
C. NGFW mode
D. FortiGuaid update servers

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 105

Refer to the exhibit.



Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

A. The session is in ESTABLISHED state.

B. The session is in FIN_ACK state.

C. The session is in SYN_SEXT state.

D. The session is in FTN_WAIT state.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 106

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

A. Web filter in flow-based inspection

B. Web application firewall

C. Application control

D. DNS filter

E. Antivirus in flow-based inspection

Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 107
Which two types of traffic are managed only by the management VDOM? (Choose two.)
A. Traffic shaping
B. PKI
C. DNS
D. FortiGuard web filter queries
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 108
A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic. In addition, the remote peer does not support a dynamic DNS update service.
What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?
A. Dialup User
B. Dynamic DNS
C. Static IP Address
D. Pre-shared Key
Answer: A (LEAVE A REPLY)

NEW QUESTION: 109
Refer to the exhibit.

Field	Value
Version	V3
Serial Number	98765432
Signature algorithm	SHA256RSA
Issuer	cn=RootCA,o=BridgeAuthority, Inc.,c=US
Valid from	Tuesday, October 3, 2016 4:33:37 PM
Valid to	Wednesday, October 2, 2019 5:03:37 PM
Subject	cn=John Doe, o=ABC, Inc.,c=US
Public key	RSA (2048 bits)
Key Usage	keyCertSign
Extended Key Usage	Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)
Basic Constraints	CA=True, Path Constraint=None
CRL Distribution Points	URL=http://webserver.abcinc.com/arlcert.crl

According to the certificate values shown in the exhibit, which type of entity was the certificate issued to?
A. A subordinate
B. A user
C. A bridge CA
D. A root CA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 110
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 private key of the CA certificate that signed the browser certificate must be installed on the browser.
B. The CA certificate that signed the web-server certificate must be installed on the browser.
C. The public key of the web server certificate must be installed on the browser.
D. The web-server certificate must be installed on the browser.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 111
Refer to the exhibit, which contains a static route configuration.

An administrator created a static route for Amazon Web Services.
What CLI command must the administrator use to view the route?
A. get router info routing-table all
B. get internet service route list
C. get router info routing-table database
D. diagnose firewall proute list
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
Refer to the exhibit.

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.

How

does FortiGate process the traffic sent to http://www.fortinet.com?

A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.

B. Traffic will be redirected to the transparent proxy and It will be allowed by proxy policy ID 1.

C. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

D. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 113

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

A. auth-on-demand

B. Idle-timeout

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

C. hard-timeout

D. soft-timeout

E. new-session

Answer: (SHOW ANSWER)

NEW QUESTION: 114

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 (LEAVE A REPLY)
Explanation
https://kb.fortinet.com/kb/documentLink.do?externalID=12069

NEW QUESTION: 115
Which three statements are true regarding session-based authentication? (Choose three.)
A. It is not recommended if multiple users are behind the source NAT
B. It requires more resources.
C. HTTP sessions are treated as a single user.
D. It can differentiate among multiple clients behind the same source IP address.
E. IP sessions from the same source IP address are treated as a single user.
Answer: (SHOW ANSWER)

NEW QUESTION: 116
An administrator has configured the following settings:

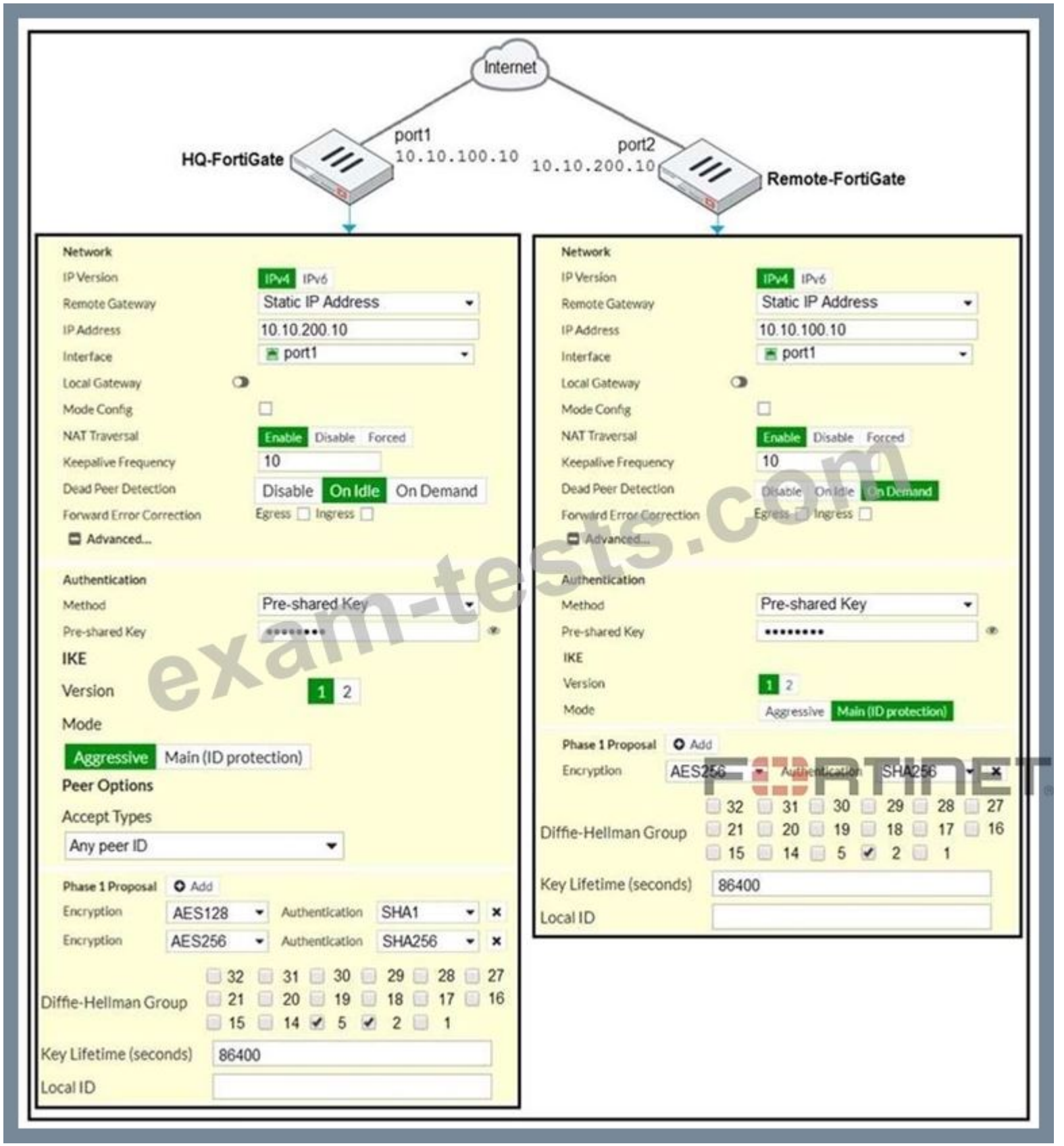
```
config system settings
set ses-denied-traffic enable
end

config system global
set block-session-timer 30
end
```


What does the configuration do? (Choose two.)
A. Reduces the amount of logs generated by denied traffic.
B. Creates a session for traffic being denied.
C. Blocks denied users for 30 minutes.
D. Enforces device detection on all interfaces for 30 minutes.
Answer: (SHOW ANSWER)

NEW QUESTION: 117
Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?
A. Global VDOM
B. FG-traffic VDOM
C. Root VDOM
D. Customer VDOM
Answer: C (LEAVE A REPLY)

NEW QUESTION: 118

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

NEW QUESTION: 119
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. Is used to discover FortiGate devices in different HA groups
D. Runs only over the heartbeat links
Answer: C,D (LEAVE A REPLY)

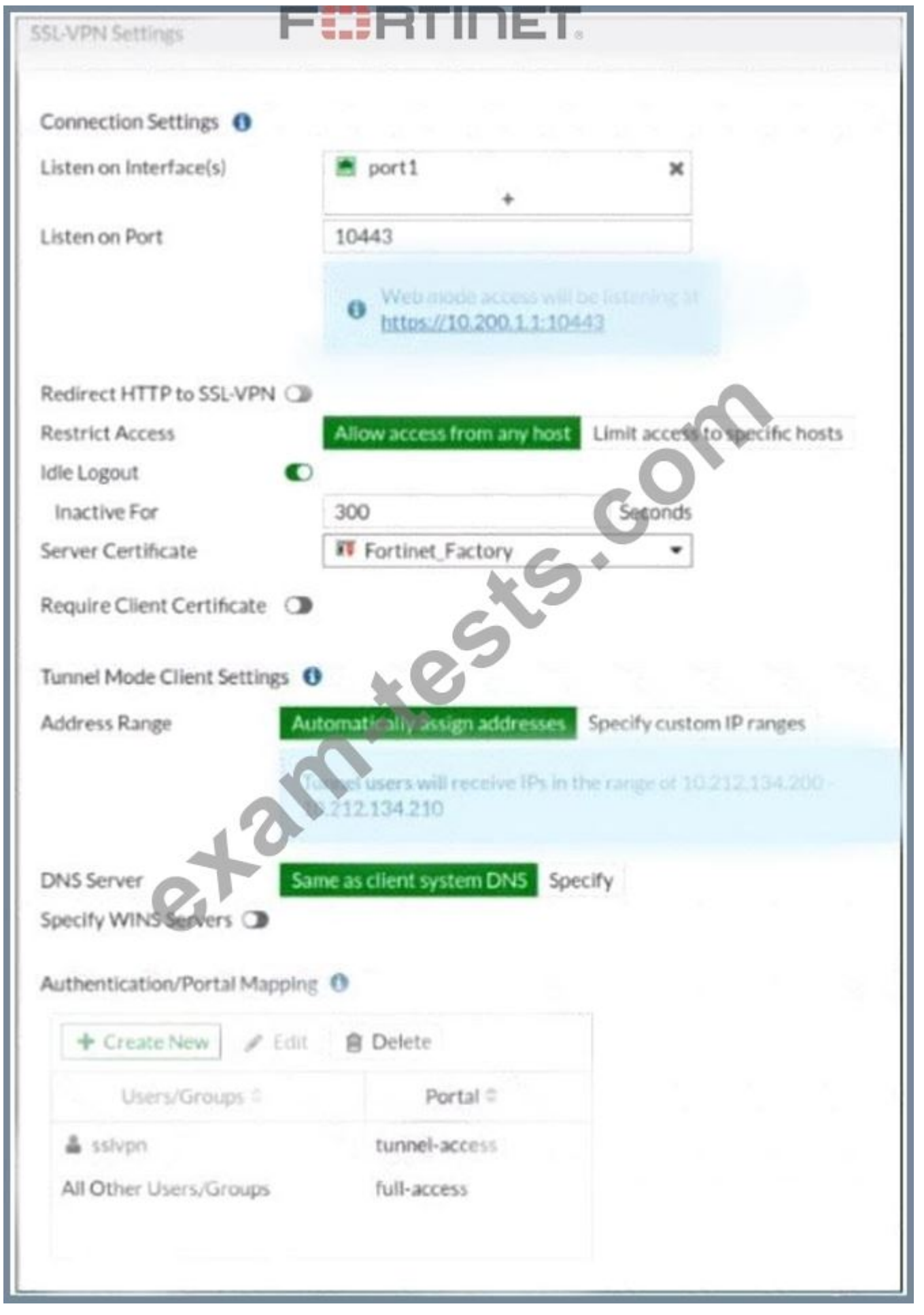
NEW QUESTION: 120
Which two inspection modes can you use to configure a firewall policy on a profile-based next-generation firewall (NGFW)? (Choose two.)
A. Proxy-based inspection
B. Full Content inspection
C. Certificate inspection
D. Flow-based inspection
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 121
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 FGVM010000064692 is the primary because of higher HA uptime.
B. FortiGate SN FGVM010000064692 has the higher HA priority.
C. FortiGate SN FGVM010000065036 HA uptime has been reset.
D. FortiGate devices are not in sync because one device is down.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 122
Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?
A. SMMIE Capabilities value
B. Subject Alternative Name value
C. Subject Key Identifier value
D. Subject value
Answer: (SHOW ANSWER)



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 Server IP address.

B. Change the idle-timeout.

C. Change the SSL VPN portal to the tunnel.

D. Change the SSL VPN port on the client.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 124

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 in TCP ESTABLISHED state.

B. The session is a bidirectional UDP connection.

C. The session is a bidirectional TCP connection.

D. The session is a UDP unidirectional state.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
Refer to the exhibit.

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

A. The session is in ESTABLISHED state.
B. The session is in SYN_SEXT state.
C. The session is in FTN_WAIT state.
D. The session is in FIN_ACK state.
Answer: (SHOW ANSWER)

NEW QUESTION: 126
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 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.

B. 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.

C. 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.

D. 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.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 127

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

https://www.fast2test.com/NSE4_FGT-6.4-practice-test.html 13

Valid Fast2test NSE4_FGT-6.4 Exam PDF Dumps - New NSE4_FGT-6.4 Real Exam Questions

A. VLAN interface

B. Software Switch interface

C. Aggregate interface

D. Redundant interface

Answer: B (LEAVE A REPLY)

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

NEW QUESTION: 128

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP

request?

A. remote user's public IP address

B. The public IP address of the FortiGate device.

C. The remote user's virtual IP address.

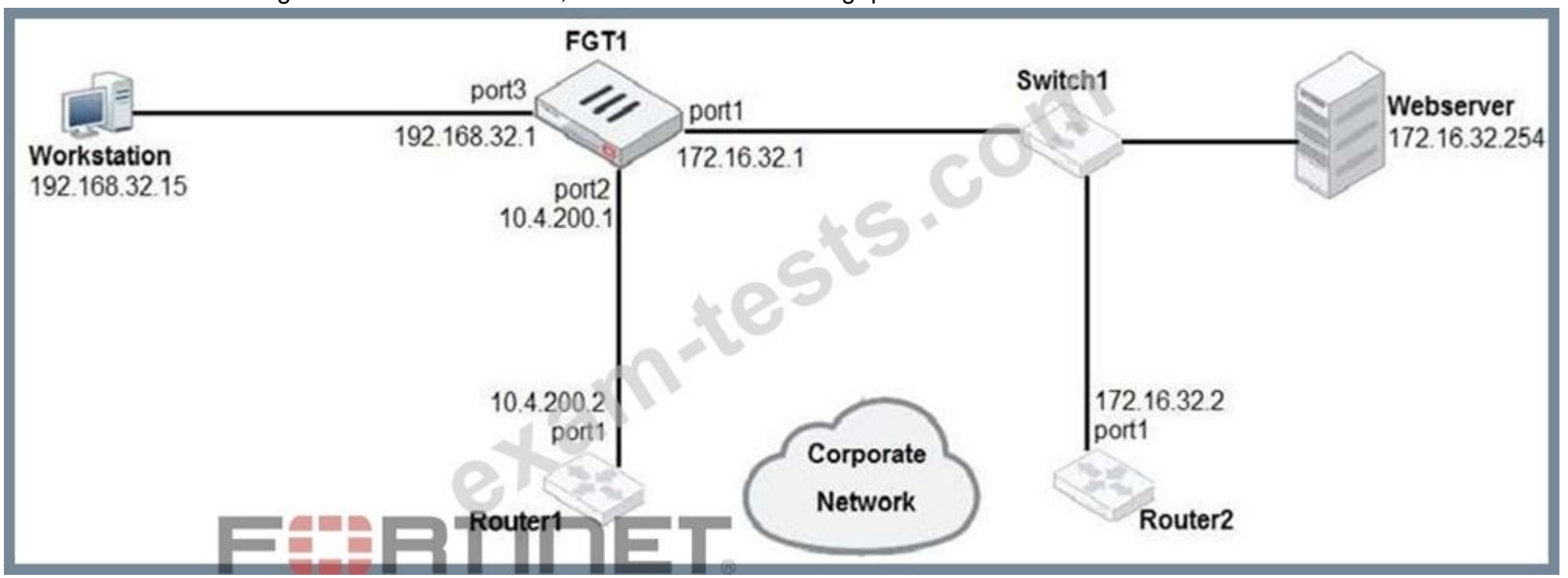
D. The internal IP address of the FortiGate device.

Answer: (SHOW ANSWER)

Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

NEW QUESTION: 129

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. 10.4.200.0/30 is directly connected, port2

B. 0.0.0.0/0 [20/0] via 10.4.200.2, port2

C. 172.16.32.0/24 is directly connected, port1

D. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]

Answer: (SHOW ANSWER)

NEW QUESTION: 130

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

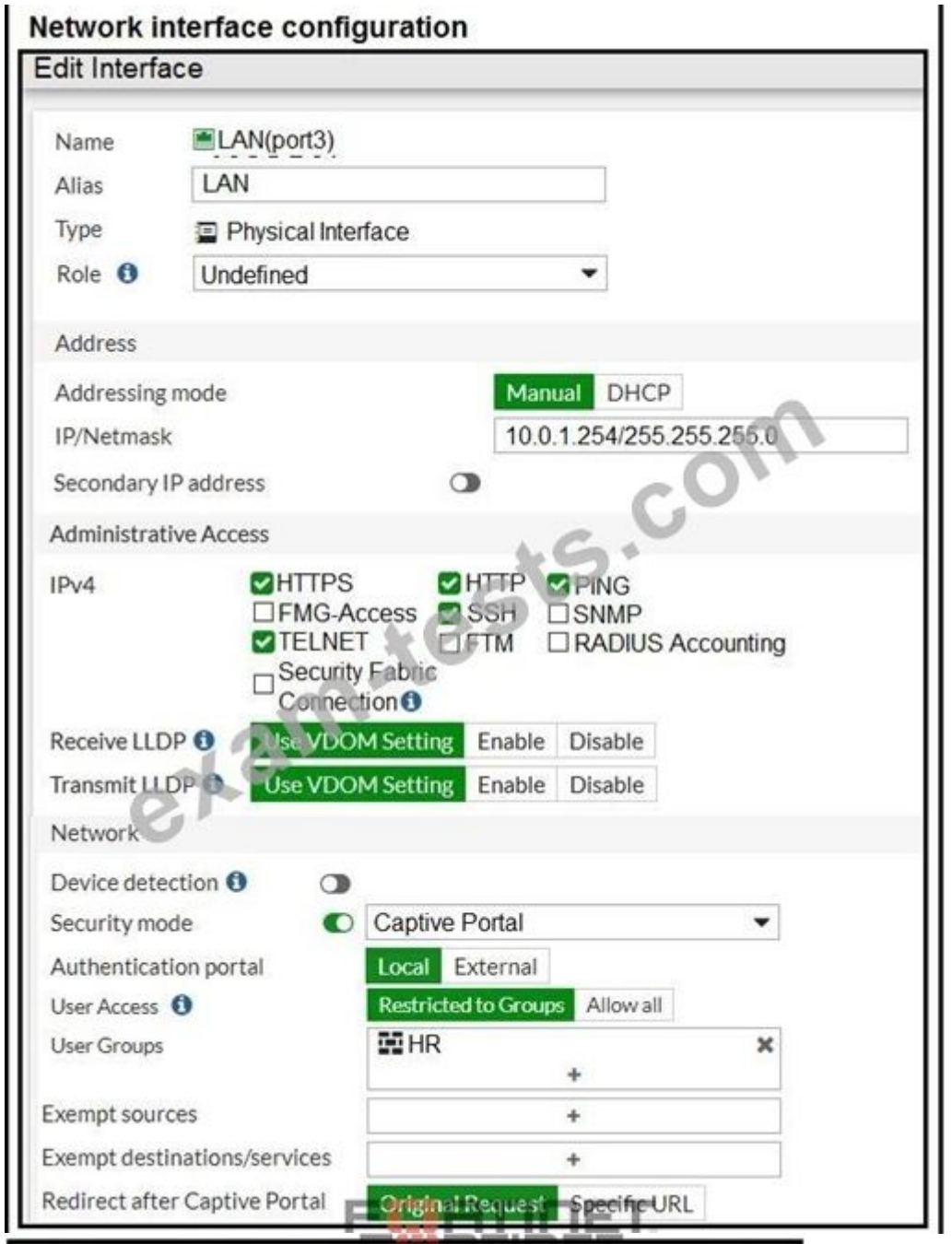
C. 192.168.1.0/24

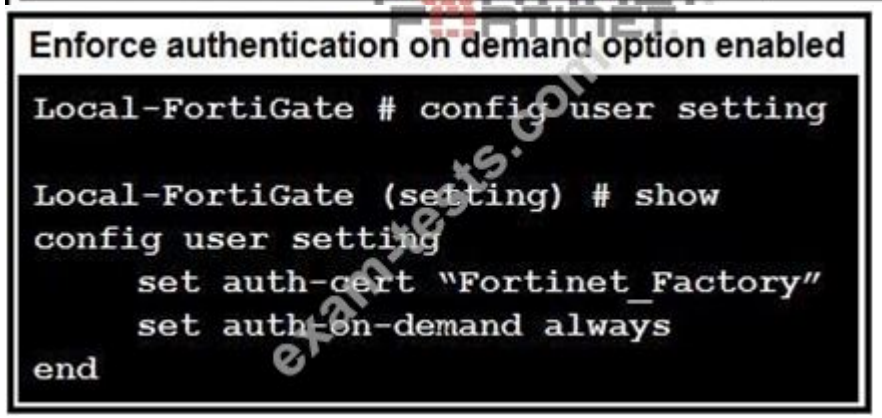
D. 192.168.0.0/8

Answer: B (LEAVE A REPLY)

NEW QUESTION: 131

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. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.

B. If there is a full-through policy in place, users will not be prompted for authentication.

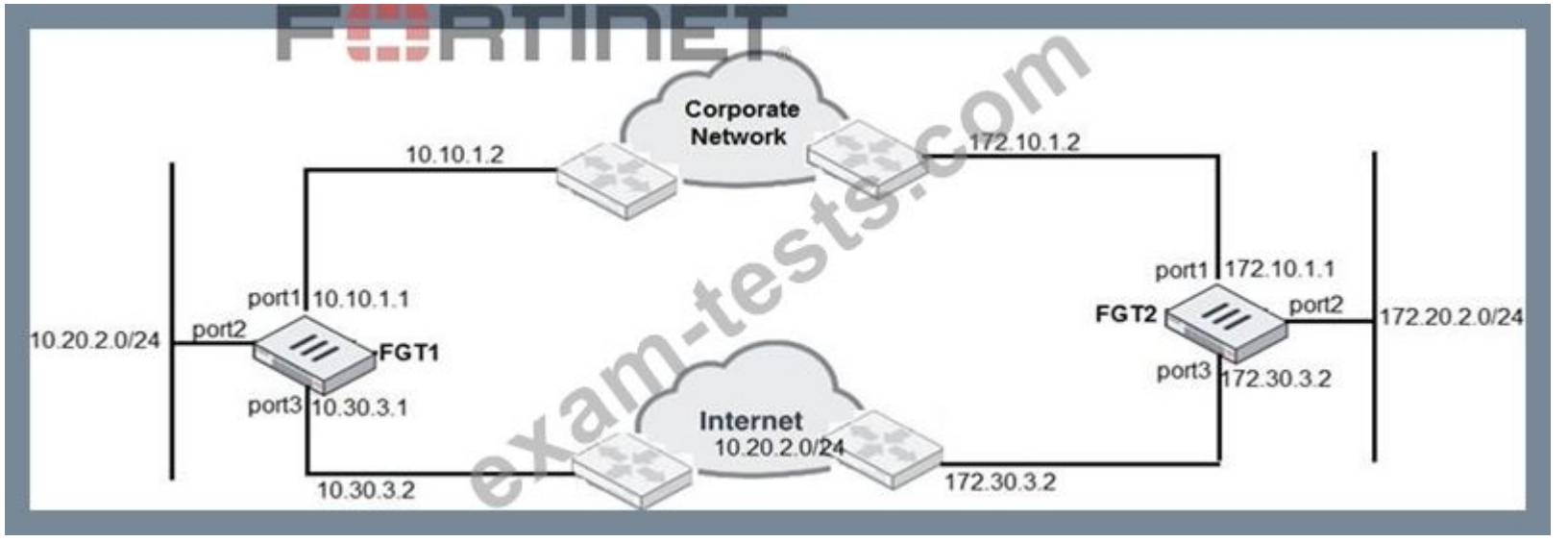
C. Authentication is enforced at a policy level; all users will be prompted for authentication.

D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 132

Examine the network diagram shown in the exhibit, and then answer the following question:



A firewall administrator must configure equal cost multipath (ECMP) routing on FGT1 to ensure both port1 and port3 links are used at the same time for all traffic destined for 172.20.2.0/24. Which of the following static routes will satisfy this requirement on FGT1? (Choose two.)

A. 172.20.2.0/24 (1/150) via 10.10.3.2, port3 [10/0]

B. 172.20.2.0/24 (1/150) via 10.30.3.2, port3 [10/0]

C. 172.20.2.0/24 (1/0) via 10.10.1.2, port1 [0/0]

D. 172.20.2.0/24 (25/0) via 10.10.3.2, port3 [5/0]

Answer: (SHOW ANSWER)

NEW QUESTION: 133

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 (LEAVE A REPLY)

NEW QUESTION: 134
Refer to the exhibit.

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.)

A. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.

B. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

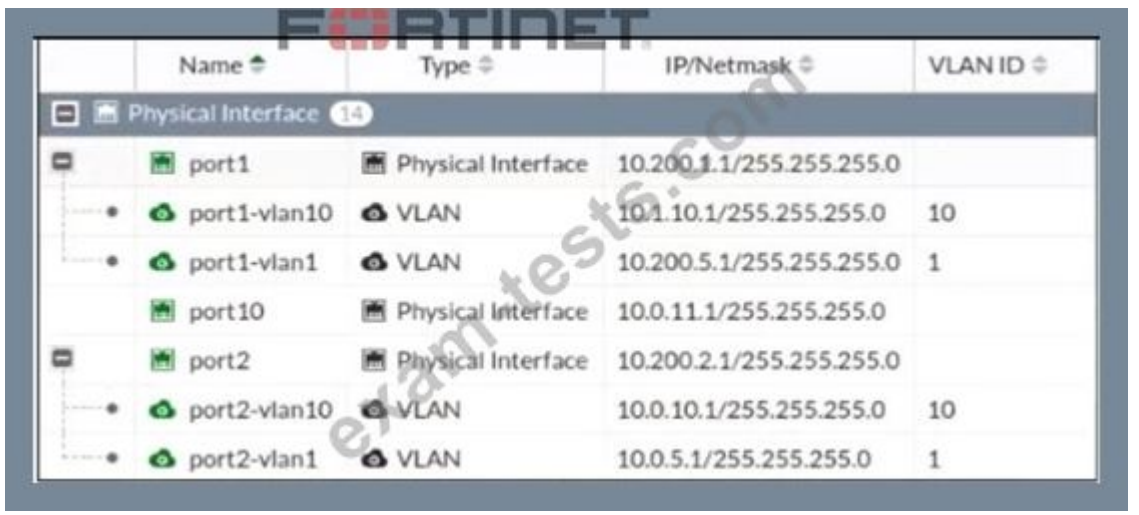
C. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.

D. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 135

Refer to the exhibit.



Given the interfaces shown in the exhibit. which two statements are true? (Choose two.)

A. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.

B. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

C. Traffic between port2 and port2-vlan1 is allowed by default.
D. port1 is a native VLAN.
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Refer to the exhibit to view the firewall policy.

Which statement is correct if well-known viruses are not being blocked?
A. The firewall policy must be configured in proxy-based inspection mode.
B. Web filter should be enabled on the firewall policy to complement the antivirus profile.
C. The firewall policy does not apply deep content inspection.
D. The action on the firewall policy must be set to deny.
Answer: C (LEAVE A REPLY)

Valid NSE4_FGT-6.4 Dumps shared by BraindumpsPass.com for Helping Passing NSE4_FGT-6.4 Exam! BraindumpsPass.com now offer the **newest NSE4_FGT-6.4 exam dumps**, the BraindumpsPass.com NSE4_FGT-6.4 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com NSE4_FGT-6.4 dumps with Test Engine here: https://www.braindumpspass.com/Fortinet/NSE4_FGT-6.4-practice-exam-dumps.html (**165** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)

Valid NSE4_FGT-6.4 Dumps shared by BraindumpsPass.com for Helping Passing NSE4_FGT-6.4 Exam! BraindumpsPass.com now offer the **newest NSE4_FGT-6.4 exam dumps**, the BraindumpsPass.com NSE4_FGT-6.4 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com NSE4_FGT-6.4 dumps with Test Engine here: https://www.braindumpspass.com/Fortinet/NSE4_FGT-6.4-practice-exam-dumps.html (**165** Q&As Dumps, **40%OFF** **Special Discount: Exam-Tests**)