Fortinet.NSE4_FGT-6.4.v2021-08-31.q50

Exam Code:	NSE4_FGT-6.4
Exam Name:	Fortinet NSE 4 - FortiOS 6.4
Certification Provider:	Fortinet
Free Question Number:	50
Version:	v2021-08-31
# of views:	377
# of Questions views:	5423
https://www.freecram.com/torrent/Fortinet.NSE4_FGT-6.4.v2021-08-31.q50.html	

NEW QUESTION: 1

An administrator needs to increase network bandwidth and provide redundancy.

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

A. VLAN interface

B. Redundant interface

C. Software Switch interface

D. Aggregate interface

Answer: D (LEAVE A REPLY)

NEW QUESTION: 2

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

B. By default, split tunneling is enabled.

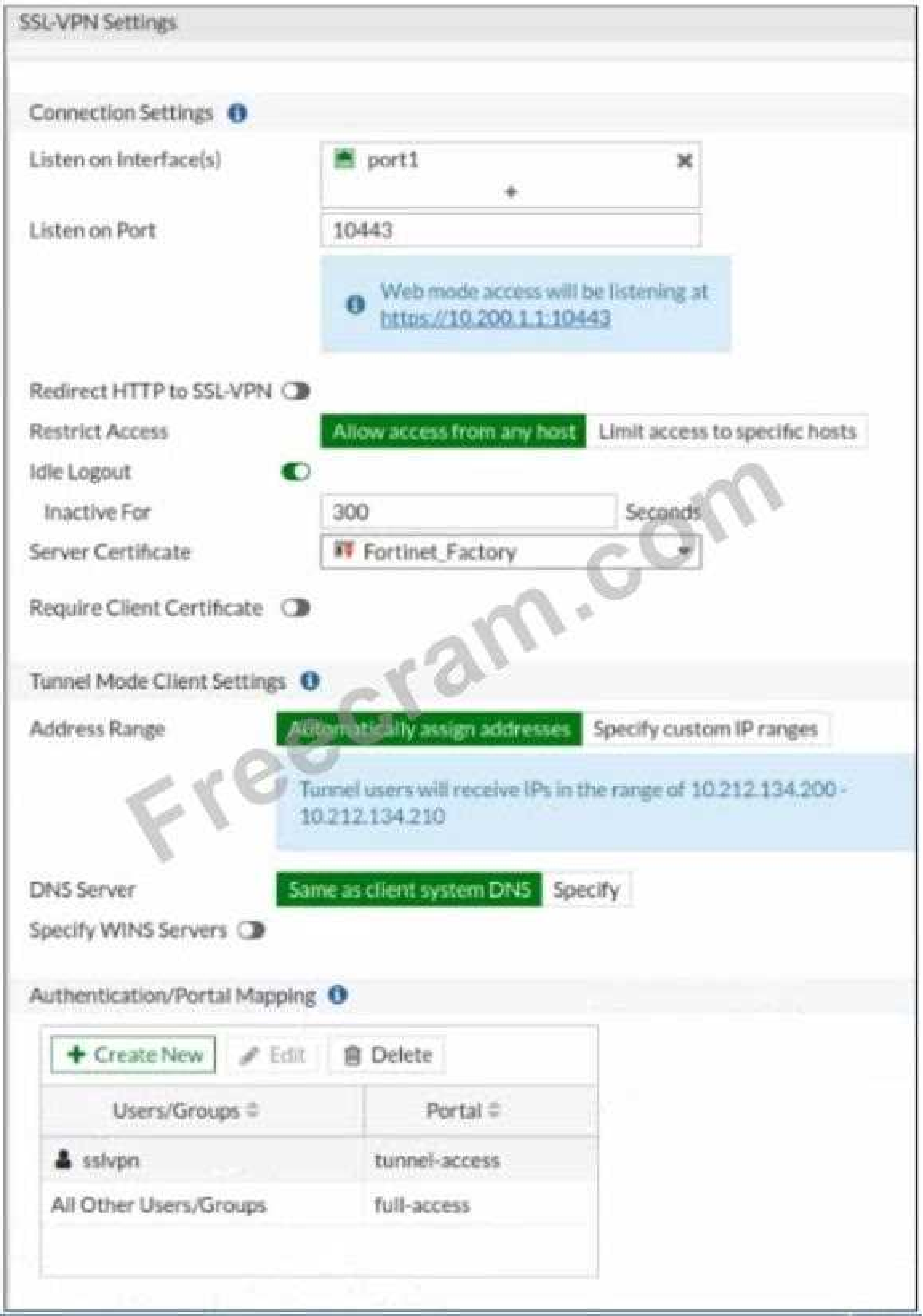
C. By default, FortiGate uses WINS servers to resolve names.

D. By default, the SSL VPN portal requires the installation of a client's certificate.

Answer: (SHOW ANSWER)

NEW QUESTION: 3

Refer to the exhibits.



SSL-VPN Settings

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

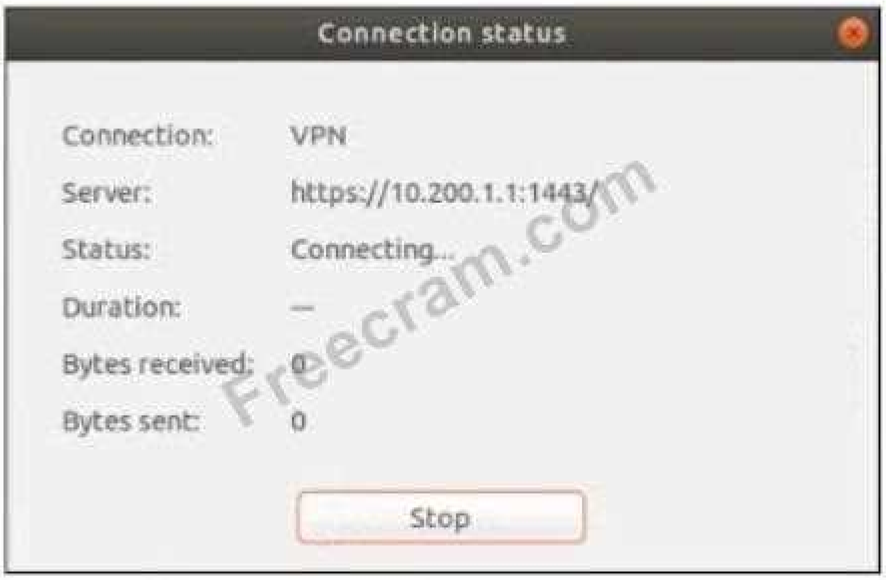
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

DNS Server: [✓ Same as client system DNS] Specify

Specify WINS Servers: ○

Authentication/Portal Mapping

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



Connection: VPN
Server: https://10.200.1.1:1443/
Status: Connecting...
Duration: --
Bytes received: 0
Bytes sent: 0

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 SSL VPN port on the client.

C. Change the idle-timeout.

D. Change the SSL VPN portal to the tunnel.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 4

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: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 5

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

A. SSH

B. HTTPS

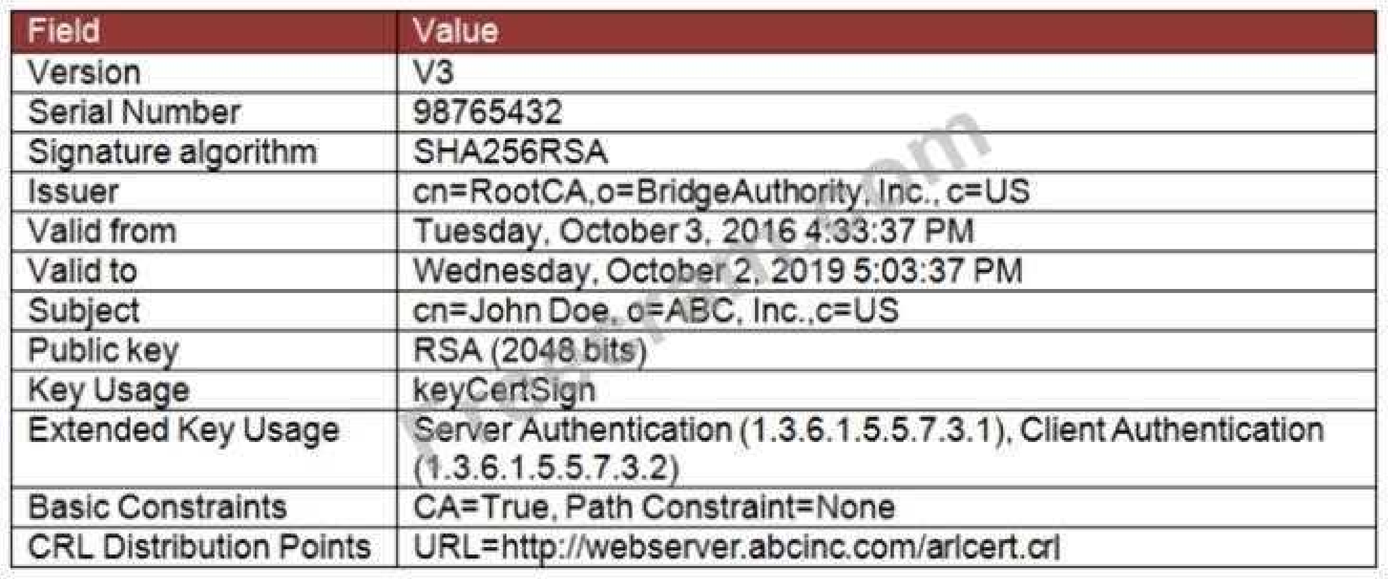
C. FortiTelemetry

D. FTM

Answer: (SHOW ANSWER)

NEW QUESTION: 6

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 user

B. A bridge CA

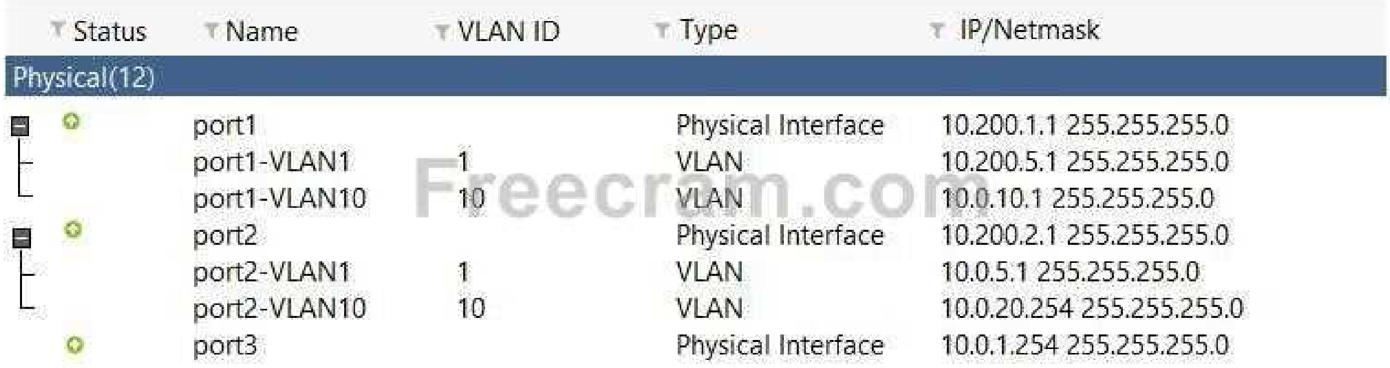
C. A subordinate

D. A root CA

Answer: A (LEAVE A REPLY)

NEW QUESTION: 7

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

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

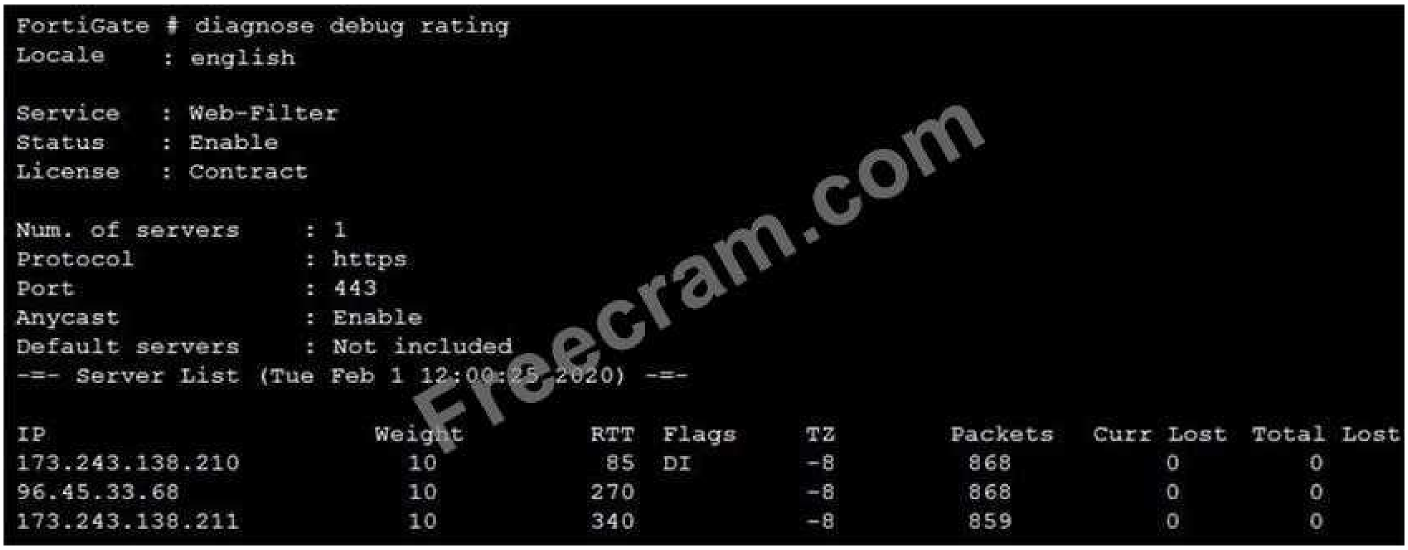
C. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.

D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 8

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

B. FortiGate is using default FortiGuard communication settings.

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

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

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 9

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 host field in the HTTP header

B. The server name indication (SNI) extension in the client hello message

C. The subject field in the server certificate

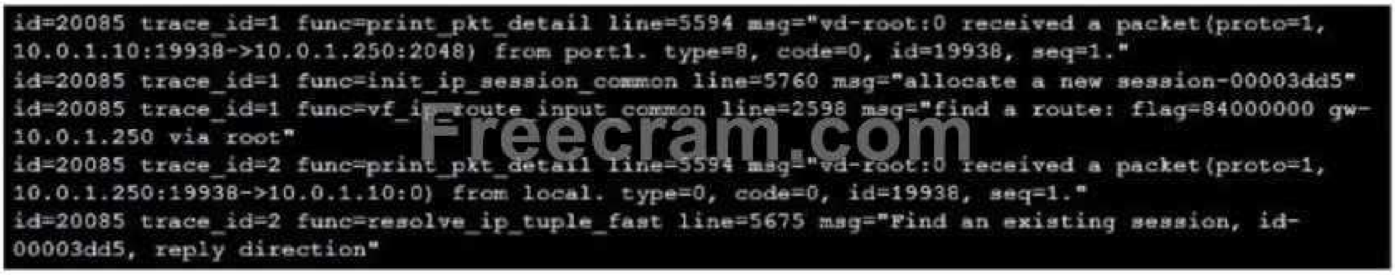
D. The serial number in the server certificate

E. The subject alternative name (SAN) field in the server certificate

Answer: (SHOW ANSWER)

NEW QUESTION: 10

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 local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id-
00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)

A. A firewall policy allowed the connection.

B. The debug flow is of ICMP traffic.

C. A new traffic session is created.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 11

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.

What is the default behavior when the local disk is full?

A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.

B. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.

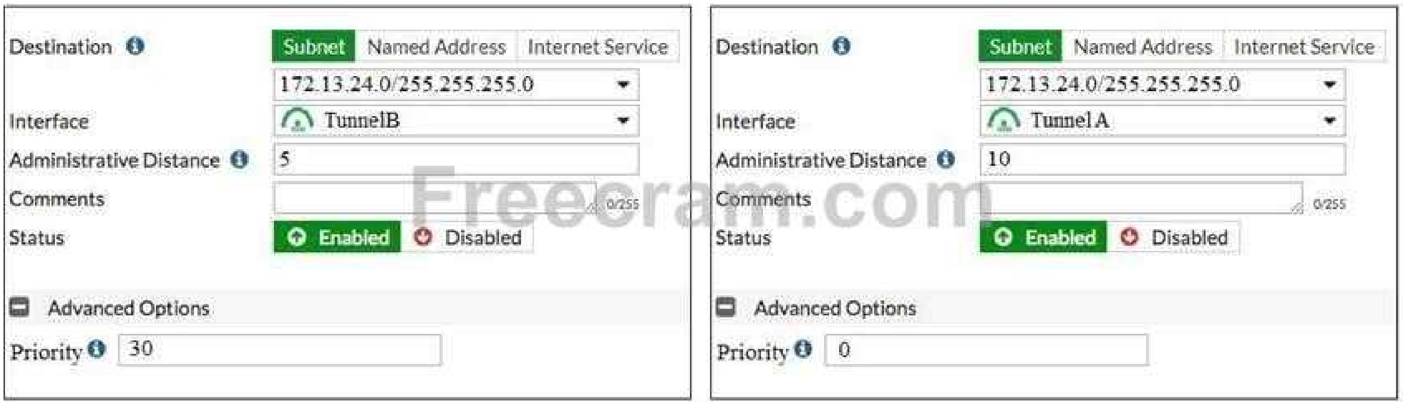
C. No new log is recorded until you manually clear logs from the local disk.

D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 12

View the exhibit.



Destination: Subnet | Named Address | Internet Service
172.13.24.0/255.255.255.0
Interface: TunnelB
Administrative Distance: 5
Comments: 0/255
Status: Enabled | Disabled
Advanced Options
Priority: 30

Destination: Subnet | Named Address | Internet Service
172.13.24.0/255.255.255.0
Interface: Tunnel A
Administrative Distance: 10
Comments: 0/255
Status: Enabled | Disabled
Advanced Options
Priority: 0

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

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

B. This is a redundant IPsec setup.

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 13

What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

A. Flow-based inspection

B. Proxy-based inspection

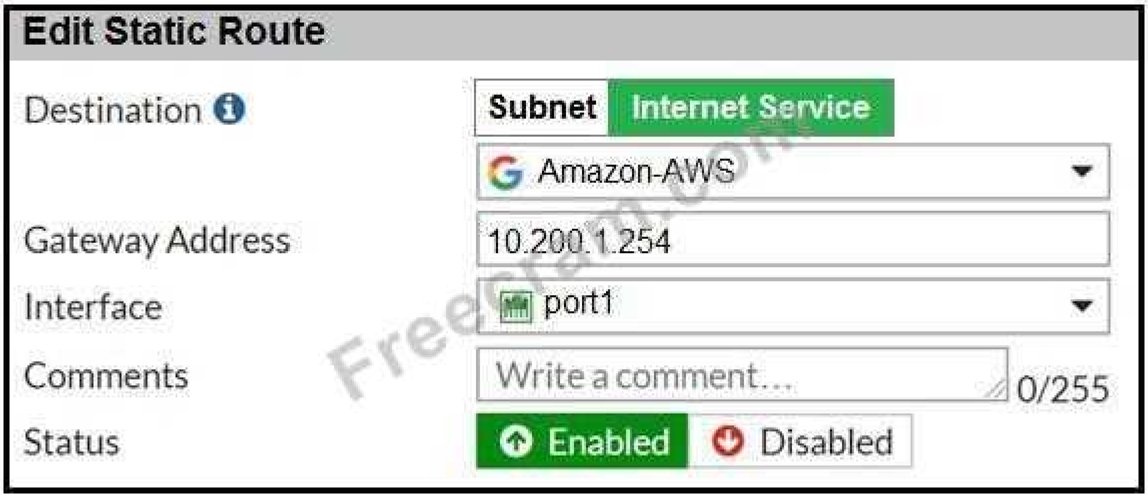
C. Full Content inspection

D. Certificate inspection

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14

Refer to the exhibit, which contains a static route configuration.



Edit Static Route

Destination: Subnet | Internet Service

Amazon-AWS

Gateway Address: 10.200.1.254

Interface: port1

Comments: Write a comment... 0/255

Status: Enabled | Disabled

An administrator created a static route for Amazon Web Services.

What CLI command must the administrator use to view the route?

A. get internet service route list

B. get router info routing-table database

C. diagnose firewall proute list

D. get router info routing-table all

Answer: C (LEAVE A REPLY)

NEW QUESTION: 15

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

A. A phase 1 SA is bidirectional, while a phase 2 SA is directional.

B. Both the phase 1 SA and phase 2 SA are bidirectional.

C. Phase 2 SA expiration can be time-based, volume-based, or both.

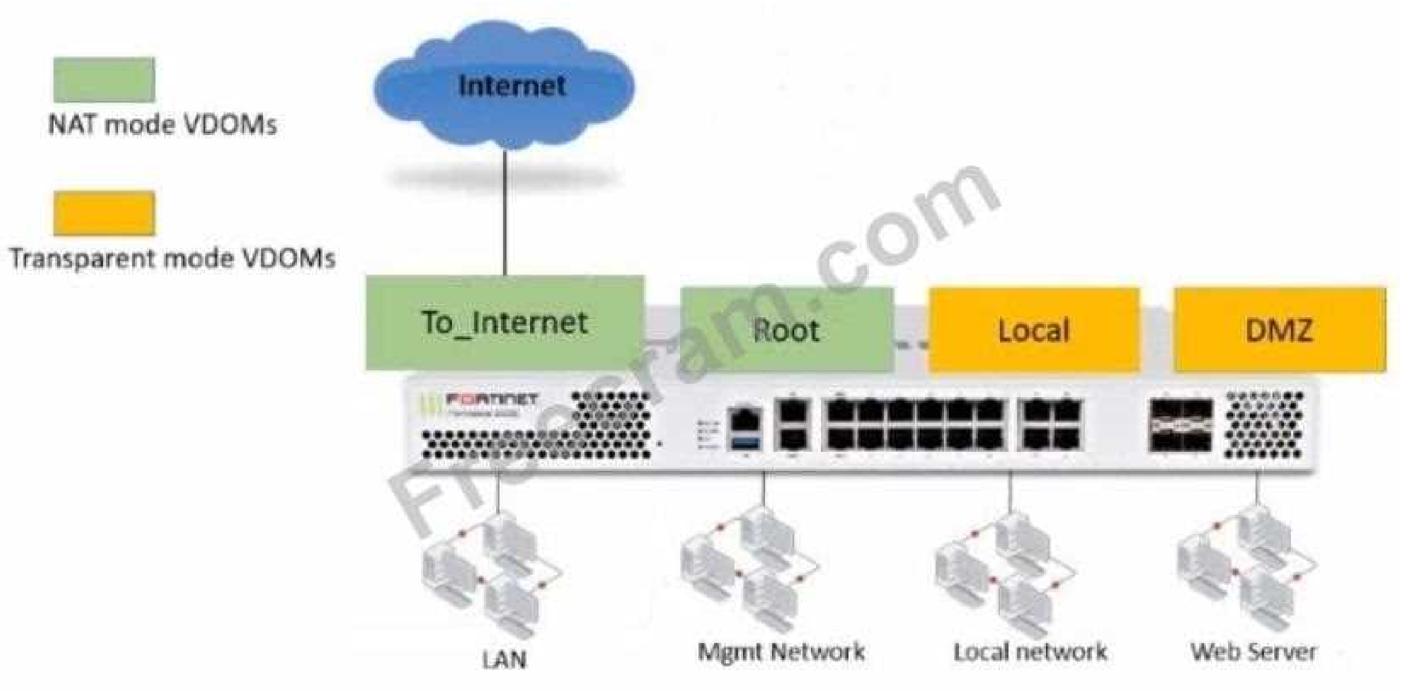
D. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.

E. An SA never expires.

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

NEW QUESTION: 16

Refer to the exhibit.



The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.

The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access 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. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 17

Which two statements are correct about SLA targets? (Choose two.)

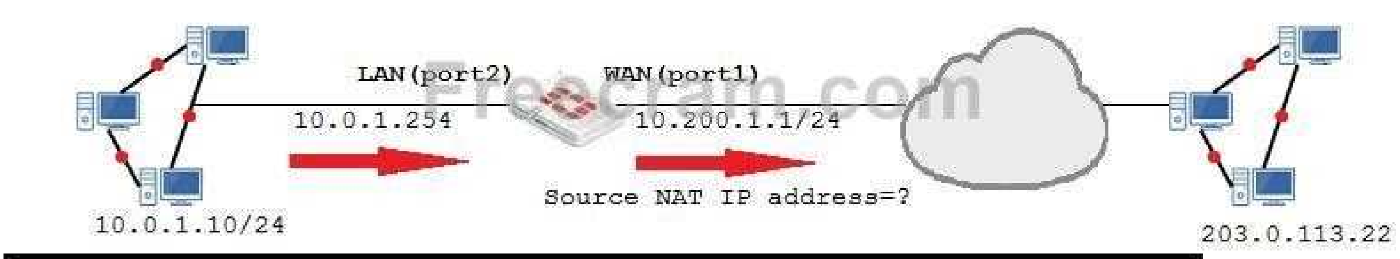
A. SLA targets are required for SD-WAN rules with a Best Quality strategy.

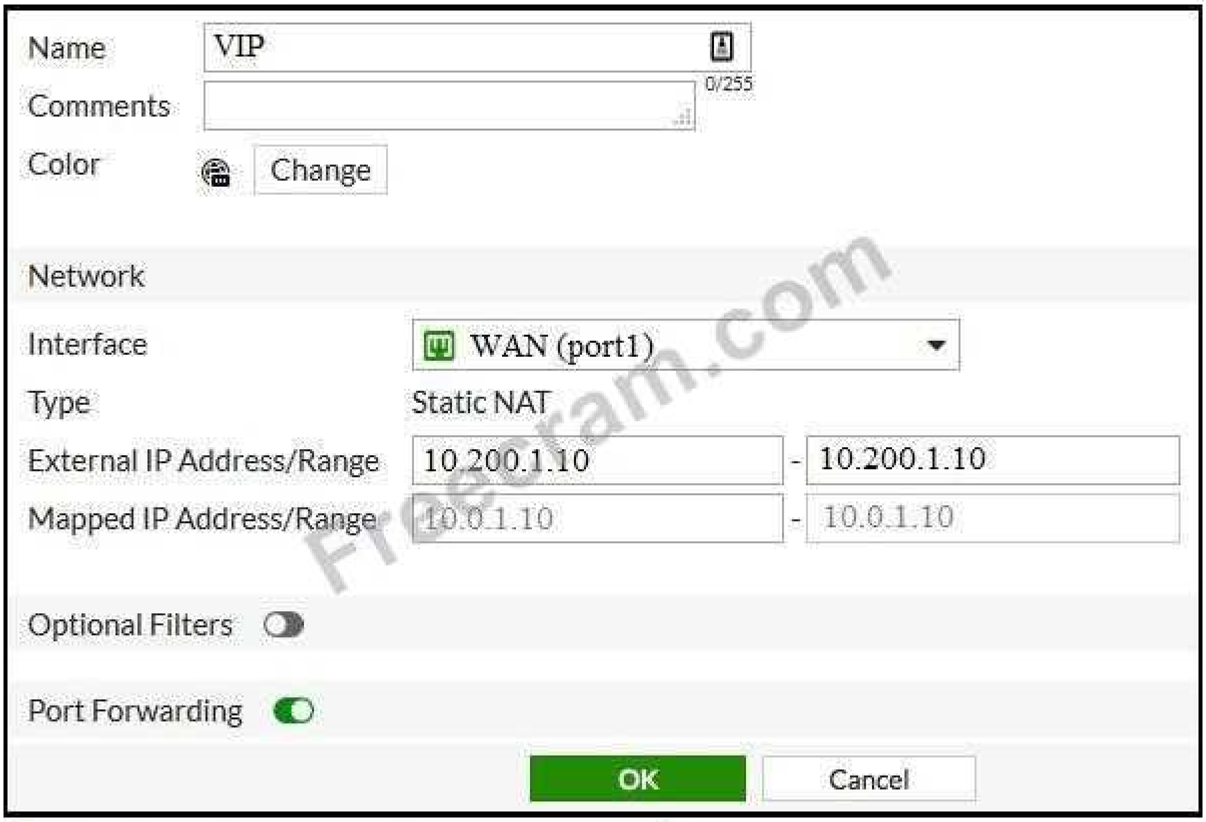
B. You can configure only two SLA targets per one Performance SLA.
C. SLA targets are used only when referenced by an SD-WAN rule.
D. SLA targets are optional.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 18

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

Network Diagram





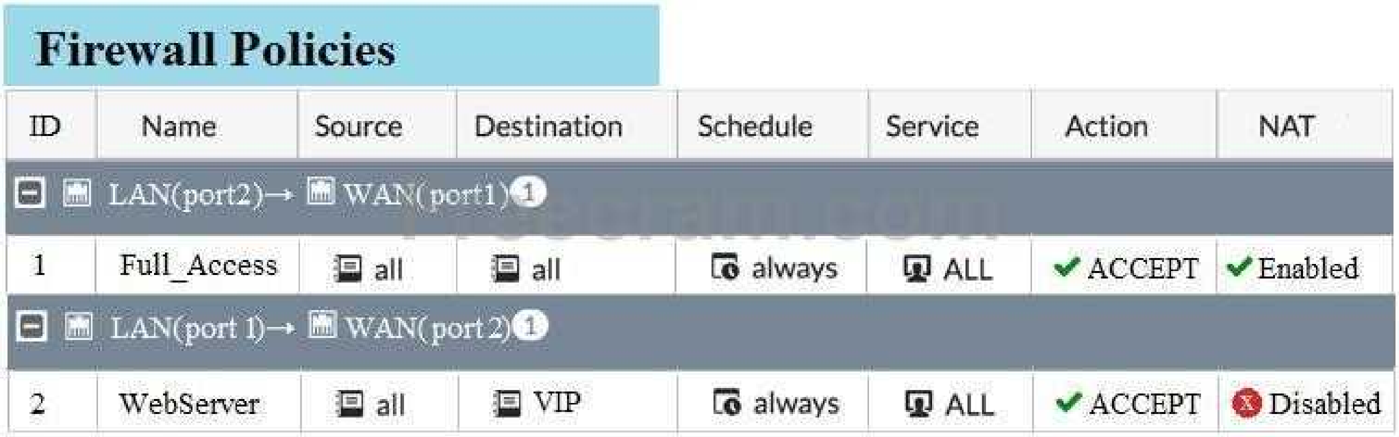
Name	VIP
Comments	0/255
Color	Change

Network

Interface	WAN (port1)	
Type	Static NAT	
External IP Address/Range	10.200.1.10	10.200.1.10
Mapped IP Address/Range	10.0.1.10	10.0.1.10

Optional Filters ○

Port Forwarding ●



Firewall Policies

ID	Name	Source	Destination	Schedule	Service	Action	NAT
⊟ LAN(port2)→ WAN(port1) 1							
1	Full_Access	all	all	always	ALL	✓ ACCEPT	✓ Enabled
⊟ LAN(port 1)→ WAN(port 2) 1							
2	WebServer	all	VIP	always	ALL	✓ ACCEPT	✗ Disabled

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

NEW QUESTION: 19
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: D (LEAVE A REPLY)
Explanation
Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

NEW QUESTION: 20
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status
B. get system arp
C. diagnose sys top
D. get system performance status
Answer: (SHOW ANSWER)

NEW QUESTION: 21
To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

A. Downstream FortiGate

B. FortiManager
C. FortiAnalyzer
D. Root FortiGate
Answer: (SHOW ANSWER)

NEW QUESTION: 22

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. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.
D. Source NAT, using central NAT, requires at least one central SNAT policy.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 23

What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)
A. Traffic to botnetservers
B. SQL injection attacks
C. Server information disclosure attacks
D. Traffic to inappropriate web sites
E. Credit card data leaks
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 24

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

NEW QUESTION: 25

Which three methods are used by the collector agent for AD polling? (Choose three.)
A. NetAPI
B. FortiGate polling
C. WMI
D. Novell API
E. WinSecLog
Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 26

Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

A. Fabric Coverage

B. Security Posture

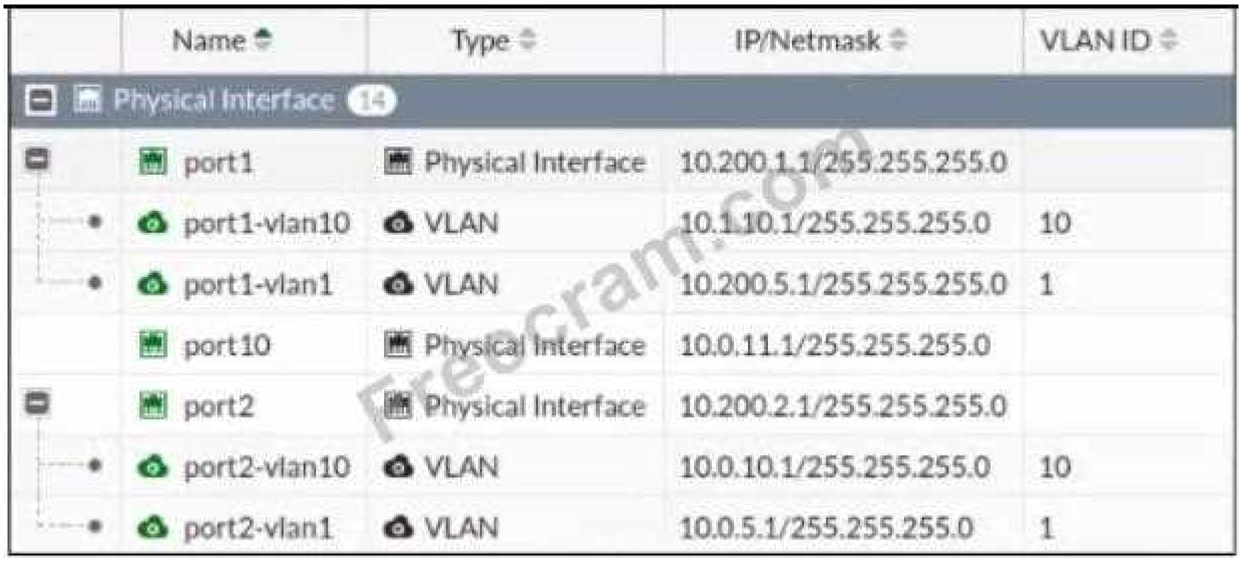
C. Optimization

D. Automated Response

Answer: B (LEAVE A REPLY)

NEW QUESTION: 27

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

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

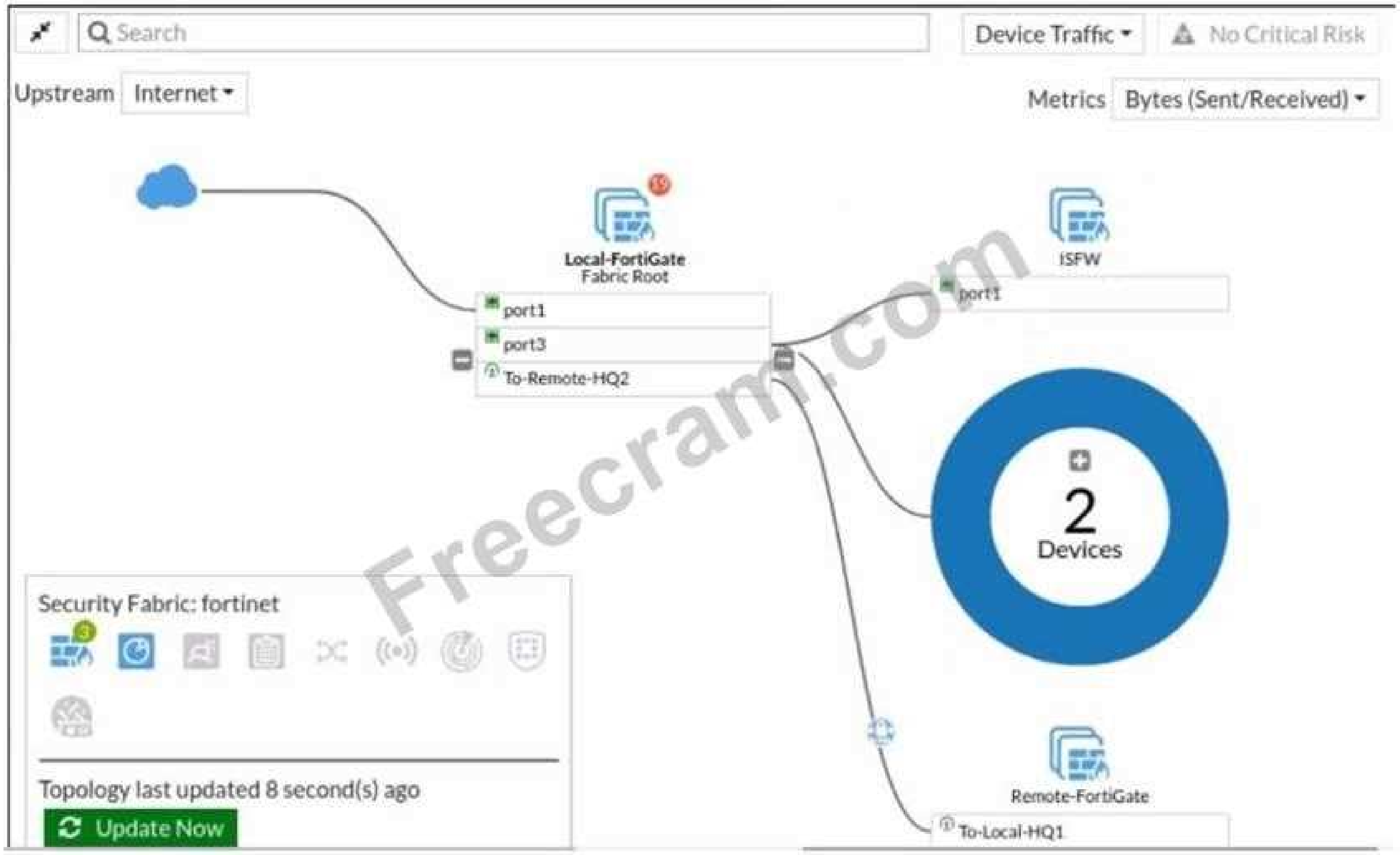
C. port1 is a native VLAN.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 28

Refer to the exhibit.



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

A. There are 19 security recommendations for the security fabric.

B. Device detection is disabled on all FortiGate devices.

C. There are five devices that are part of the security fabric.

D. This security fabric topology is a logical topology view.

Answer: (SHOW ANSWER)

NEW QUESTION: 29

Which two statements are true about collector agent standard access mode? (Choose two.)

A. Standard mode security profiles apply to organizational units (OU).

B. Standard mode uses Windows convention-NetBios: Domain\Username.

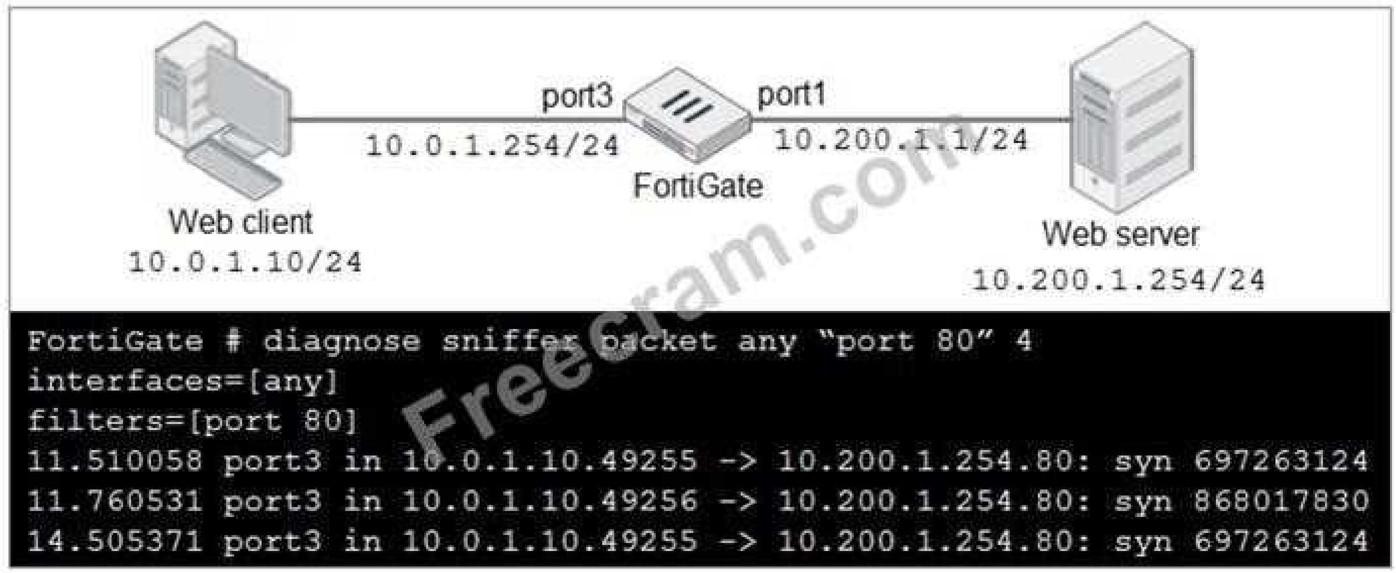
C. Standard mode security profiles apply to user groups.

D. Standard access mode supports nested groups.

Answer: (SHOW ANSWER)

NEW QUESTION: 30

Refer to the exhibit.



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

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

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

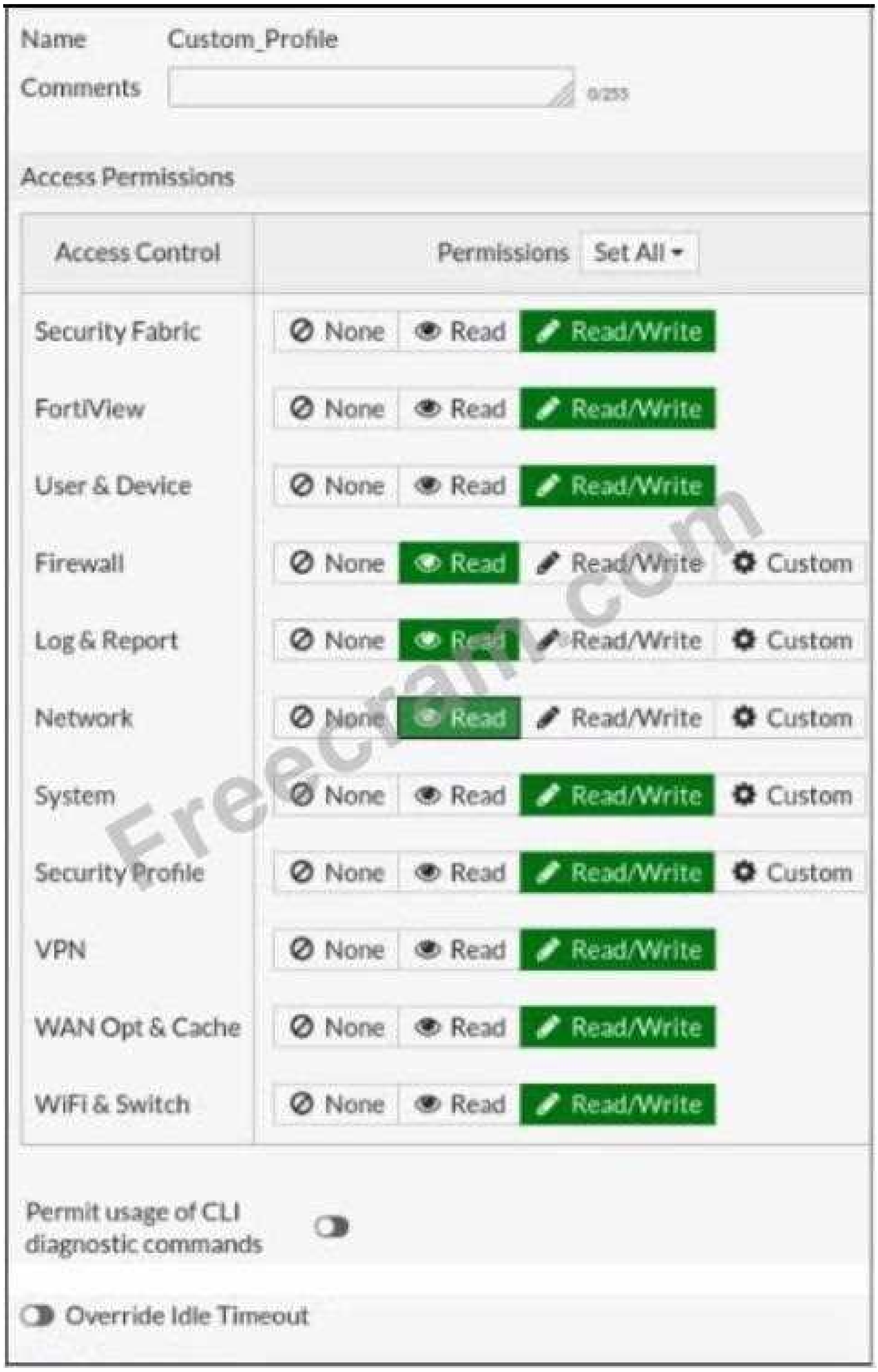
NEW QUESTION: 31

What is the primary FortiGate election process when the HA override setting is disabled?

A. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
B. Connected monitored ports > System uptime > Priority > FortiGate Serial number
C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
D. Connected monitored ports > Priority > System uptime > FortiGate Serial number
Answer: A (LEAVE A REPLY)

NEW QUESTION: 32

Refer to the exhibit.



Name Custom_Profile

Comments 0/255

Access Permissions

Access Control	Permissions Set All ▾
Security Fabric	None Read [✓ Read/Write]
FortiView	None Read [✓ Read/Write]
User & Device	None Read [✓ Read/Write]
Firewall	None [✓ Read] Read/Write Custom
Log & Report	None [✓ Read] Read/Write Custom
Network	None [✓ Read] Read/Write Custom
System	None Read [✓ Read/Write] Custom
Security Profile	None Read [✓ Read/Write] Custom
VPN	None Read [✓ Read/Write]
WAN Opt & Cache	None Read [✓ Read/Write]
WiFi & Switch	None Read [✓ Read/Write]

Permit usage of CLI diagnostic commands ○

○ Override Idle Timeout

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: D (LEAVE A REPLY)

NEW QUESTION: 33

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. 192.168.1.0/24

B. 192.168.0.0/8

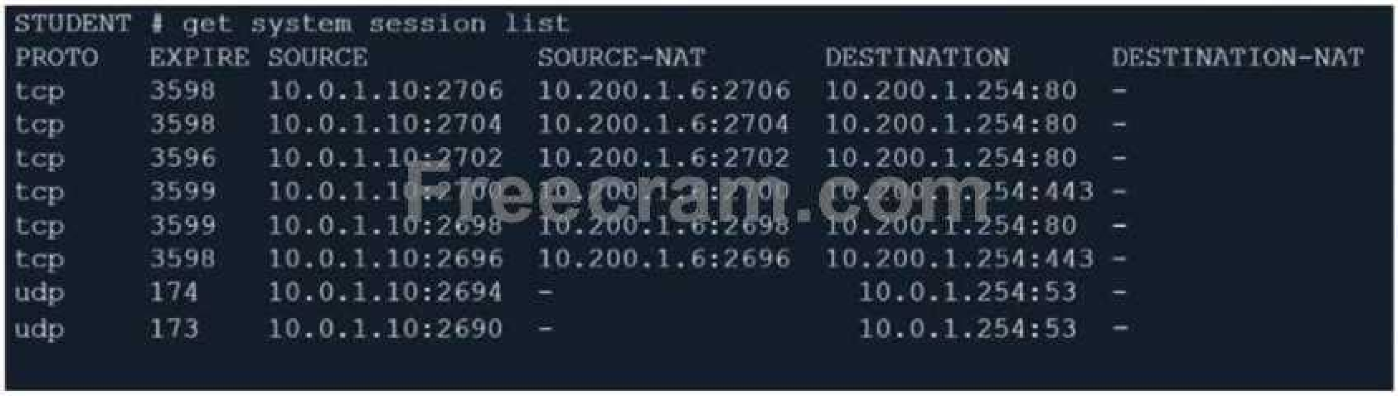
C. 192.168.2.0/24

D. 192.168.3.0/24

Answer: C (LEAVE A REPLY)

NEW QUESTION: 34

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

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

C. Destination NAT is disabled in the firewall policy.

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 35

NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

A. Web filtering

B. Antivirus

C. Application control

D. Web proxy

Answer: B (LEAVE A REPLY)

NEW QUESTION: 36

Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)

A. Root
B. FG-traffic
C. FG-Mgmt
D. Mgmt
Answer: (SHOW ANSWER)

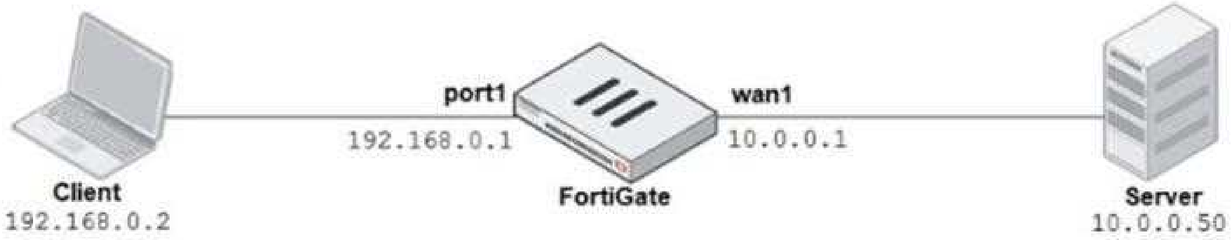
NEW QUESTION: 37

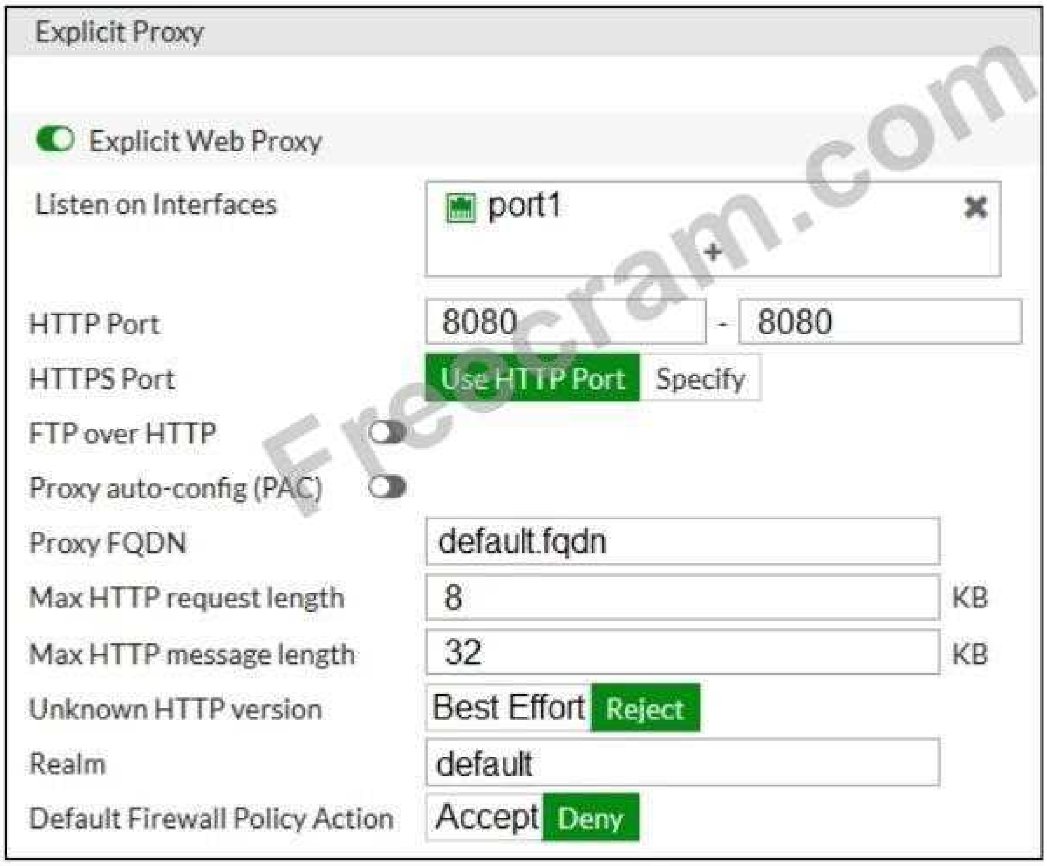
Which statement about the policy ID number of a firewall policy is true?

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

NEW QUESTION: 38

Refer to the exhibit.





Explicit Proxy

● Explicit Web Proxy

Listen on Interfaces	port1
HTTP Port	8080 - 8080
HTTPS Port	[✓ Use HTTP Port] Specify
FTP over HTTP	○
Proxy auto-config (PAC)	○
Proxy FQDN	default.fqdn
Max HTTP request length	8 KB
Max HTTP message length	32 KB
Unknown HTTP version	Best Effort [✓ Reject]
Realm	default
Default Firewall Policy Action	Accept [✓ Deny]

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 192.168.0.2 and port 8080'
B. 'host 10.0.0.50 and port 8080'
C. 'host 192.168.0.1 and port 80'
D. 'host 10.0.0.50 and port 80'
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.
C. Lowest to highest policy ID number.
D. Services defined in the firewall policy.
E. Highest to lowest priority defined in the firewall policy.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 40
Which two statements about antivirus scanning mode are true? (Choose two.)

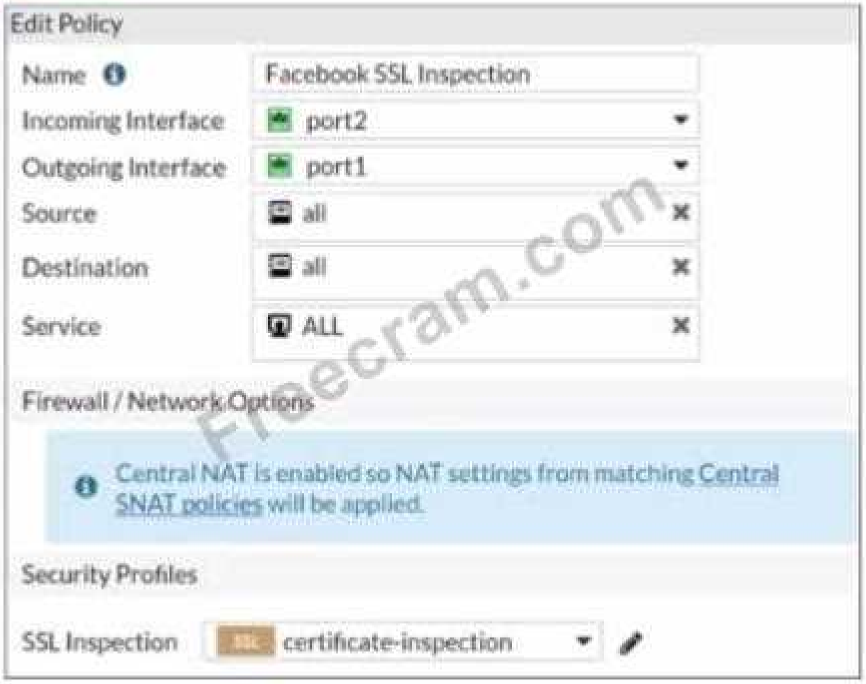
A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
B. In flow-based inspection mode, files bigger than the buffer size are scanned.
C. In flow-based inspection mode. FortiGate buffers the file, but also simultaneously transmits it to the client.
D. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 41
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 first packet from the session originator
B. Lookup is done on the last packet sent from the responder
C. Lookup is done on the trust reply packet from the responder
D. Lookup is done on every packet, regardless of direction
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 42
Refer to the exhibits.

Exhibit A



Edit Policy

Name: Facebook SSL Inspection

Incoming Interface: port2

Outgoing Interface: port1

Source: all

Destination: all

Service: ALL

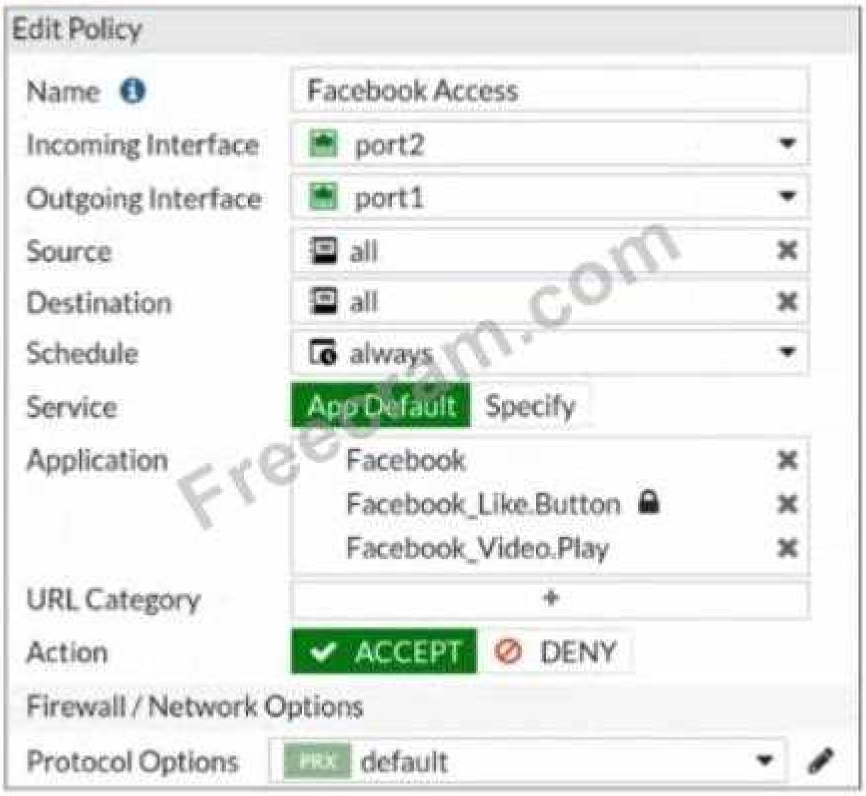
Firewall / Network Options

Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.

Security Profiles

SSL Inspection: SSL certificate-inspection

Exhibit B



Edit Policy

Name: Facebook Access

Incoming Interface: port2

Outgoing Interface: port1

Source: all

Destination: all

Schedule: always

Service: App Default | Specify

Application: Facebook, Facebook_Like.Button, Facebook_Video.Play

URL Category: +

Action: ✓ ACCEPT | ⊘ DENY

Firewall / Network Options

Protocol Options: PRX default

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) tor Facebook.

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

A. Force access to Facebook using the HTTP service.

B. Additional application signatures are required to add to the security policy.

C. The SSL inspection needs to be a deep content inspection.

D. Add Facebook in the URL category in the security policy.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 43

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

* All traffic must be routed through the primary tunnel when both tunnels are up

* The secondary tunnel must be used only if the primary tunnel goes down

* In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

B. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

C. Enable Dead Peer Detection.

D. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 44

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. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.

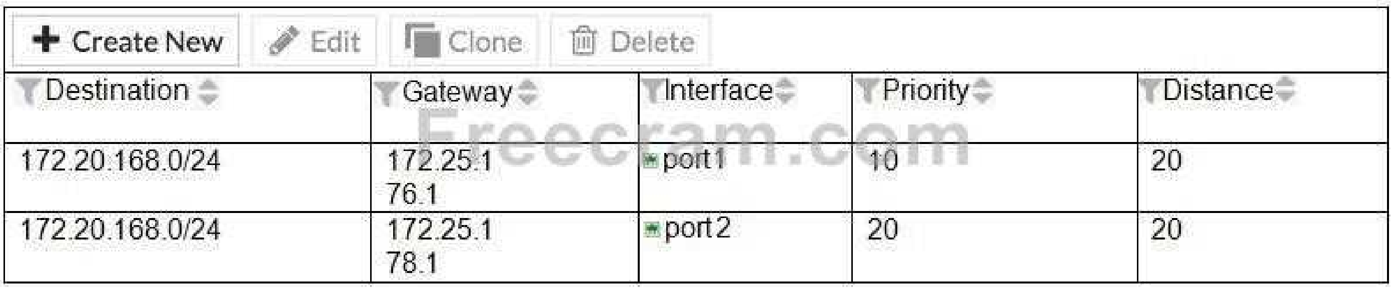
C. It provides executive summaries of the four largest areas of security focus.

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

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 45

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



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

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

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

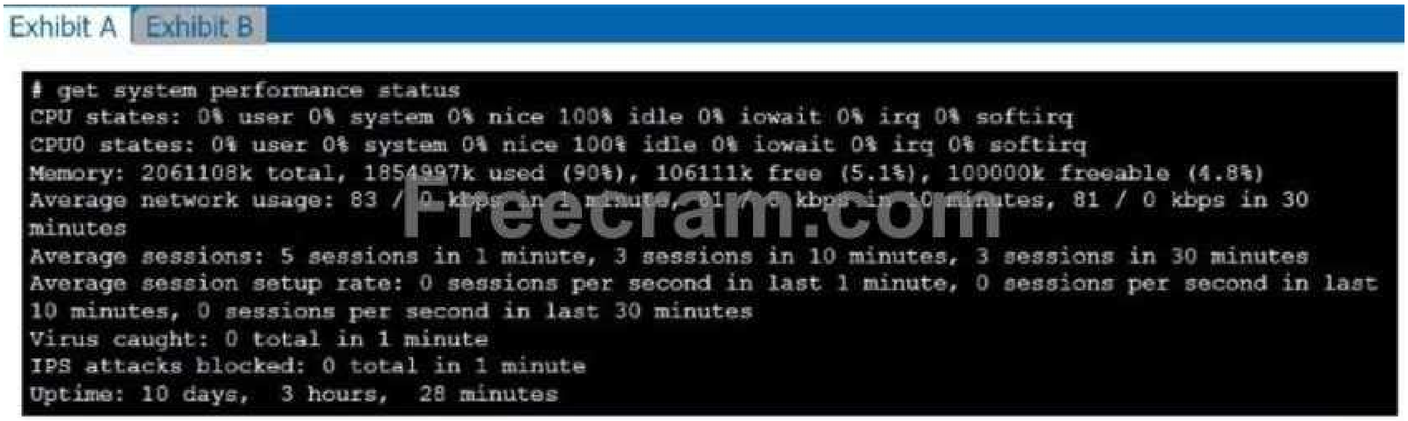
Answer: B (LEAVE A REPLY)

Explanation

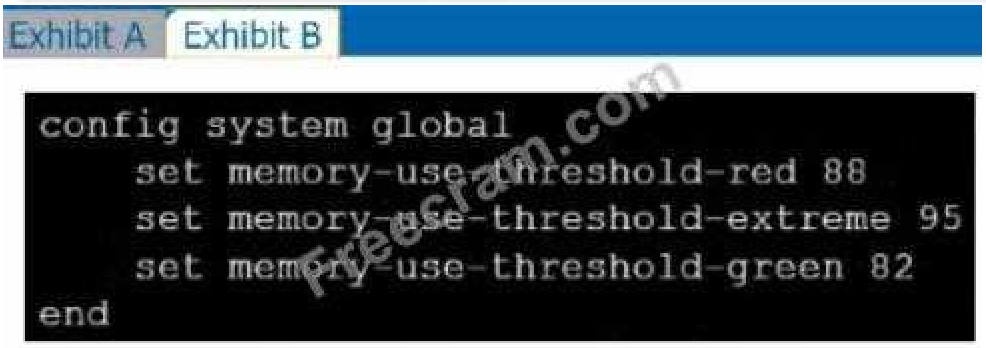
"If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path."

NEW QUESTION: 46

Refer to the exhibits.



```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 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
```



```
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 cannot change the configuration.

B. FortiGate has entered conserve mode.

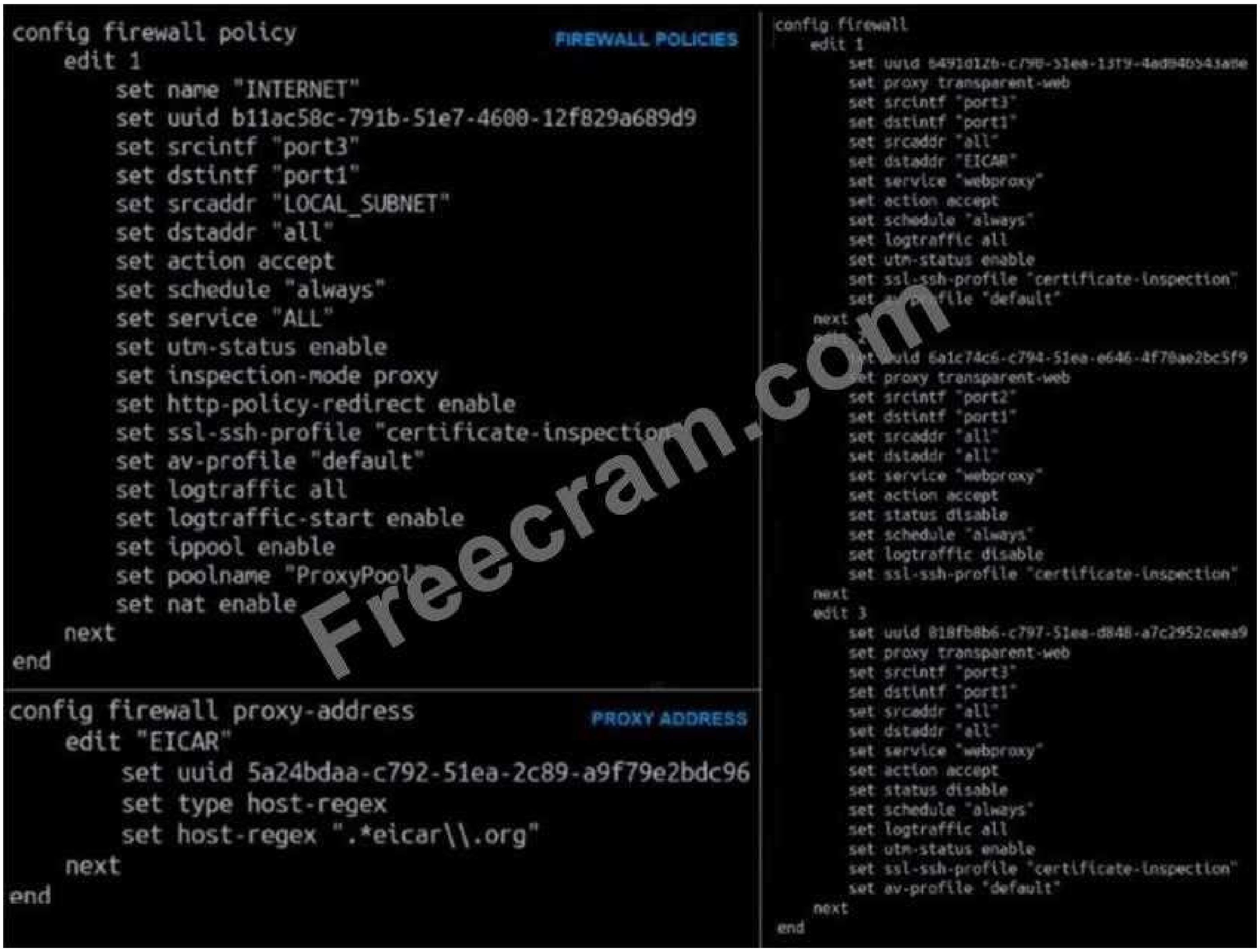
C. Administrators can access FortiGate only through the console port.

D. FortiGate will start sending all files to FortiSandbox for inspection.

Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 47

Refer to the exhibit.



```
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
```

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

```
config firewall
    edit 1
        set uuid b491d12b-c790-51ea-13f9-4ad94b543a0e
        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 not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.

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

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: (SHOW ANSWER)

NEW QUESTION: 48

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

A. Lowest to highest policy ID number.

B. Services defined in the firewall policy.

C. Source defined as Internet Services in the firewall policy.

D. Destination defined as Internet Services in the firewall policy.

E. Highest to lowest priority defined in the firewall policy.

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

NEW QUESTION: 49

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.

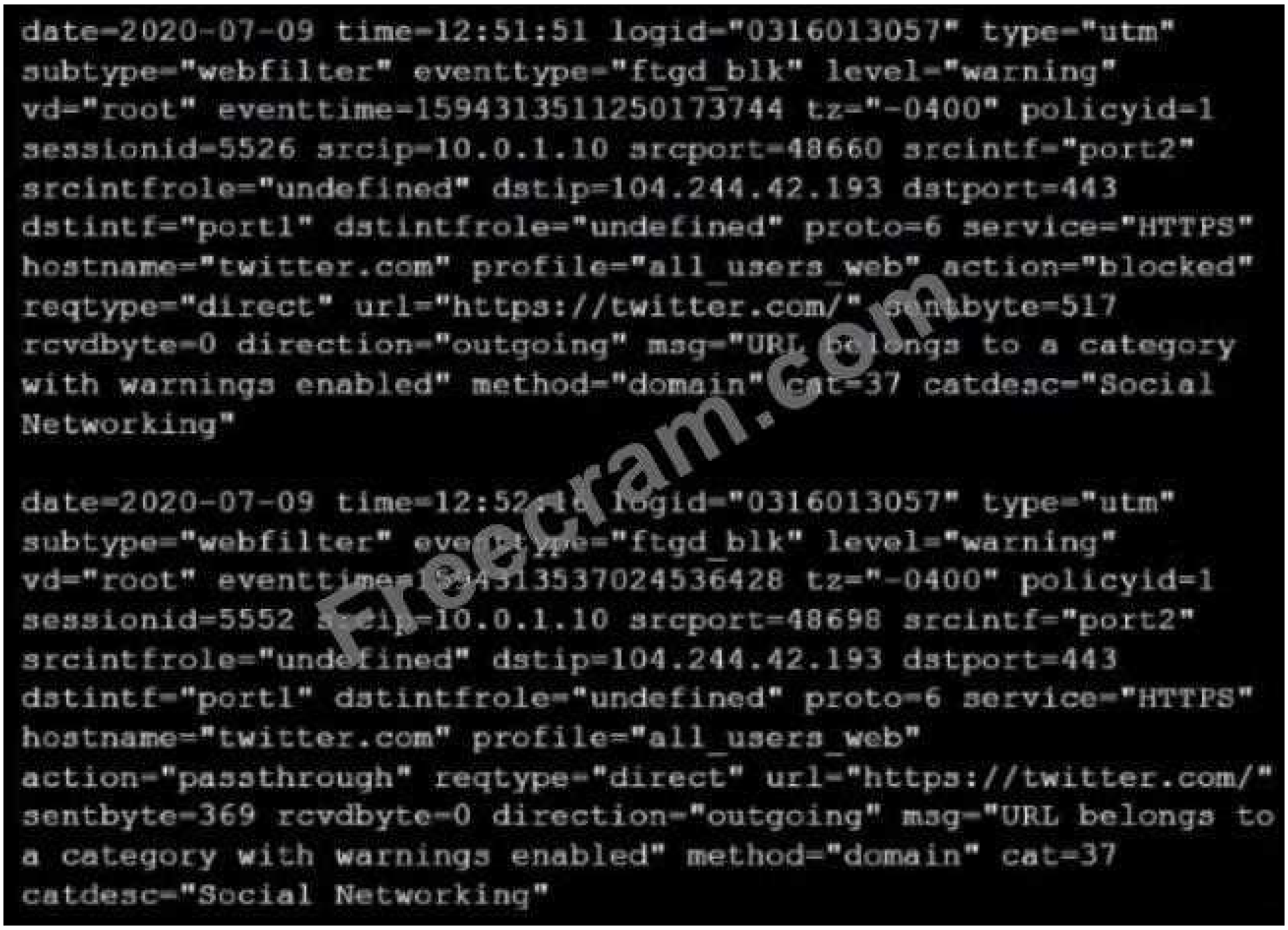
C. Tunnels are negotiated dynamically between spokes.

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: A,C (LEAVE A REPLY)

NEW QUESTION: 50

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=12:52:17 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. 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. The name of the firewall policy is all_users_web.

Answer: A (LEAVE A REPLY)