Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

NEW QUESTION 1
An administrator wants to simplify remote access without asking users to provide user credentials. Which access control method provides this solution?

A. ZTNA IP/MAC filtering mode
B. ZTNA access proxy
C. SSL VPN
D. L2TP

Answer: B

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.165): "ZTNA access proxy allows users to securely access resources through an SSL-encrypted access proxy. This simplifies remote access by eliminating the use of VPNs."
This is true because ZTNA access proxy is a feature that allows remote users to access internal applications without requiring VPN or user credentials. ZTNA access proxy uses a secure tunnel between the user’s device and the FortiGate, and authenticates the user based on device identity and context. The user only needs to install a lightweight agent on their device, and the FortiGate will automatically assign them to the appropriate application group based on their device profile. This simplifies remote access and enhances security by reducing the attack surface12

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

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

Answer: D

NEW QUESTION 3
An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192. 168. 1.0/24 and the remote quick mode selector is 192. 168.2.0/24.
Which subnet must the administrator configure for the local quick mode selector for site B?

A. 192. 168. 1.0/24
B. 192. 168.0.0/24
C. 192. 168.2.0/24
D. 192. 168.3.0/24

Answer: C

Explanation:
For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.
To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.
Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

NEW QUESTION 4
Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
B. The RPF check is run on the first sent and reply packet of any new session.
C. The RPF check is run on the first sent packet of any new session.
D. The RPF check is run on the first reply packet of any new session.

Answer: AC

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.41): "The RPF check is a mechanism that protects FortiGate and your network from IP spoofing attacks by checking for a return path to the source in the routing table." "FortiGate performs an RPF check only on the first packet of a new session. That is, after the first packet passes the RPF check and FortiGate accepts the session, FortiGate doesn’t perform any additional RPF checks on that session."
* A. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.
This is true because the RPF check verifies that the source IP address of an incoming packet matches the reverse route for that address, meaning that the packet came from a legitimate source and not from an attacker who is trying to impersonate another host. This prevents IP spoofing attacks, where an attacker sends packets with a forged source IP address to bypass security policies or launch denial-of-service attacks1
* C. The RPF check is run on the first sent packet of any new session.
This is true because the RPF check is performed only once per session, on the first packet sent by either the client or the server, depending on the direction of the session initiation. This reduces the processing overhead and improves performance2

NEW QUESTION 5
An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

A. Policy lookup will be disabled.
B. By Sequence view will be disabled.
C. Search option will be disabled

D. Interface Pair view will be disabled.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821

NEW QUESTION 6
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time
B. FortiGuaid update servers
C. Operating mode
D. NGFW mode

Answer: CD

Explanation:
C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.
D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

NEW QUESTION 7
Examine this PAC file configuration.
Which of the following statements are true? (Choose two.)

A. Browsers can be configured to retrieve this PAC file from the FortiGate.
B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.
C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
D. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 8
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

A. diagnose sys top
B. execute ping
C. execute traceroute
D. diagnose sniffer packet any
E. get system arp

Answer: BCD

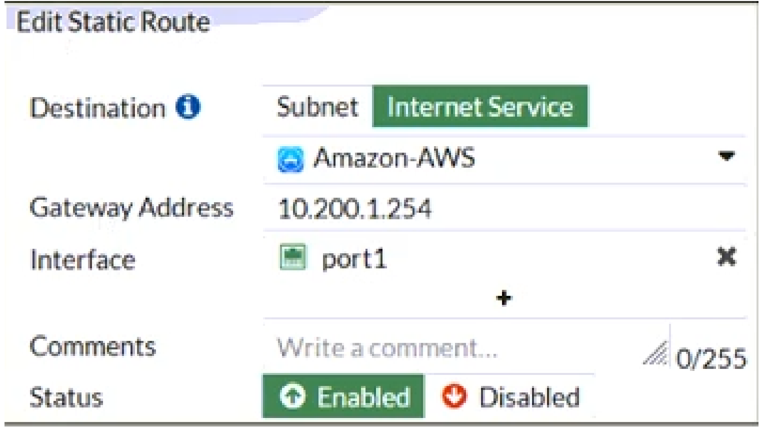
NEW QUESTION 9
Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

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

Answer: AD

Explanation:
"In order for FortiGate to act in these roles, its CA certificate must have the basic constraints extension set to cA=True and the value of the keyUsage extension set to keyCertSign."

NEW QUESTION 10
Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.



Edit Static Route

Destination ℹ Subnet **Internet Service**

Amazon-AWS

Gateway Address 10.200.1.254

Interface port1 ✖

+

Comments Write a comment... 0/255

Status **Enabled** Disabled

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

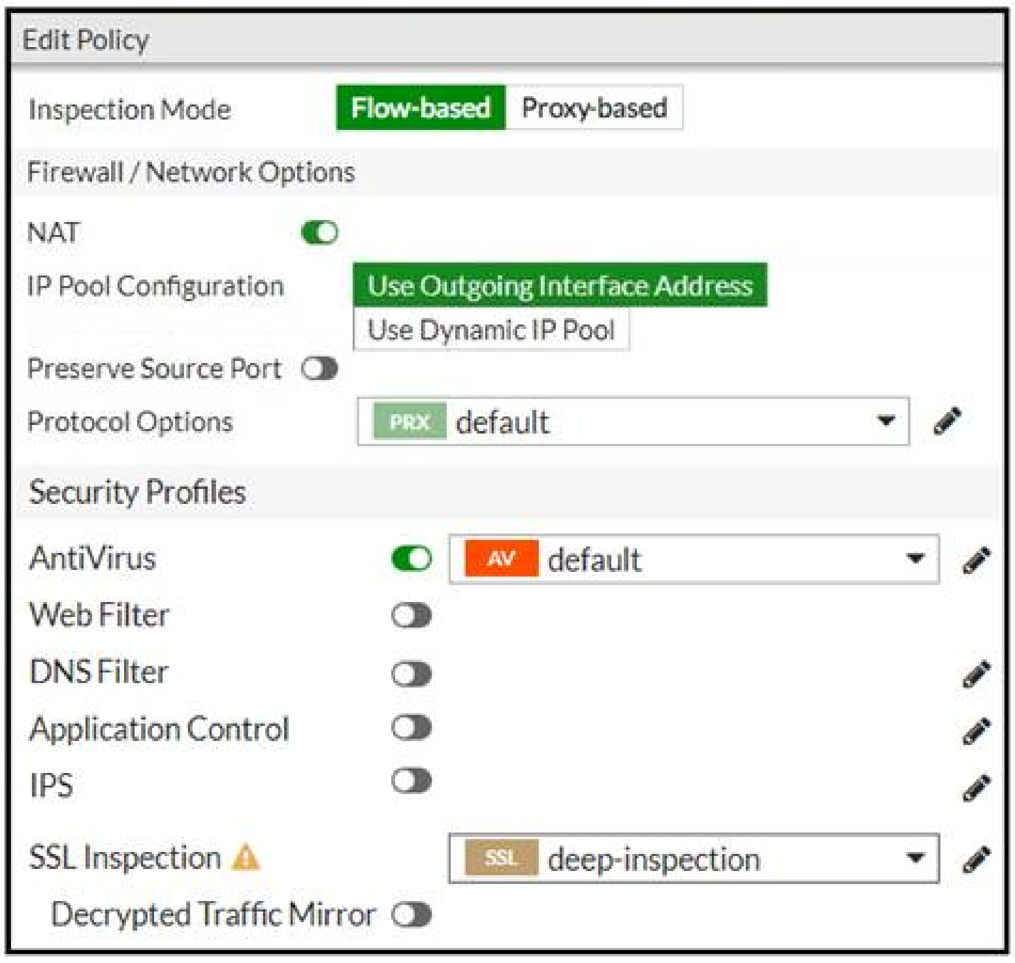
A. get router info routing-table database
B. diagnose firewall route list
C. get internet-service route list

D. get router info routing-table all

Answer: B

Explanation:
ISDB static route will not create entry directly in routing-table. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1
and here
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640
FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

NEW QUESTION 10
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).



Edit Policy

Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT ●

IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool

Preserve Source Port ○

Protocol Options: PRX default

Security Profiles

AntiVirus ● AV default

Web Filter ○

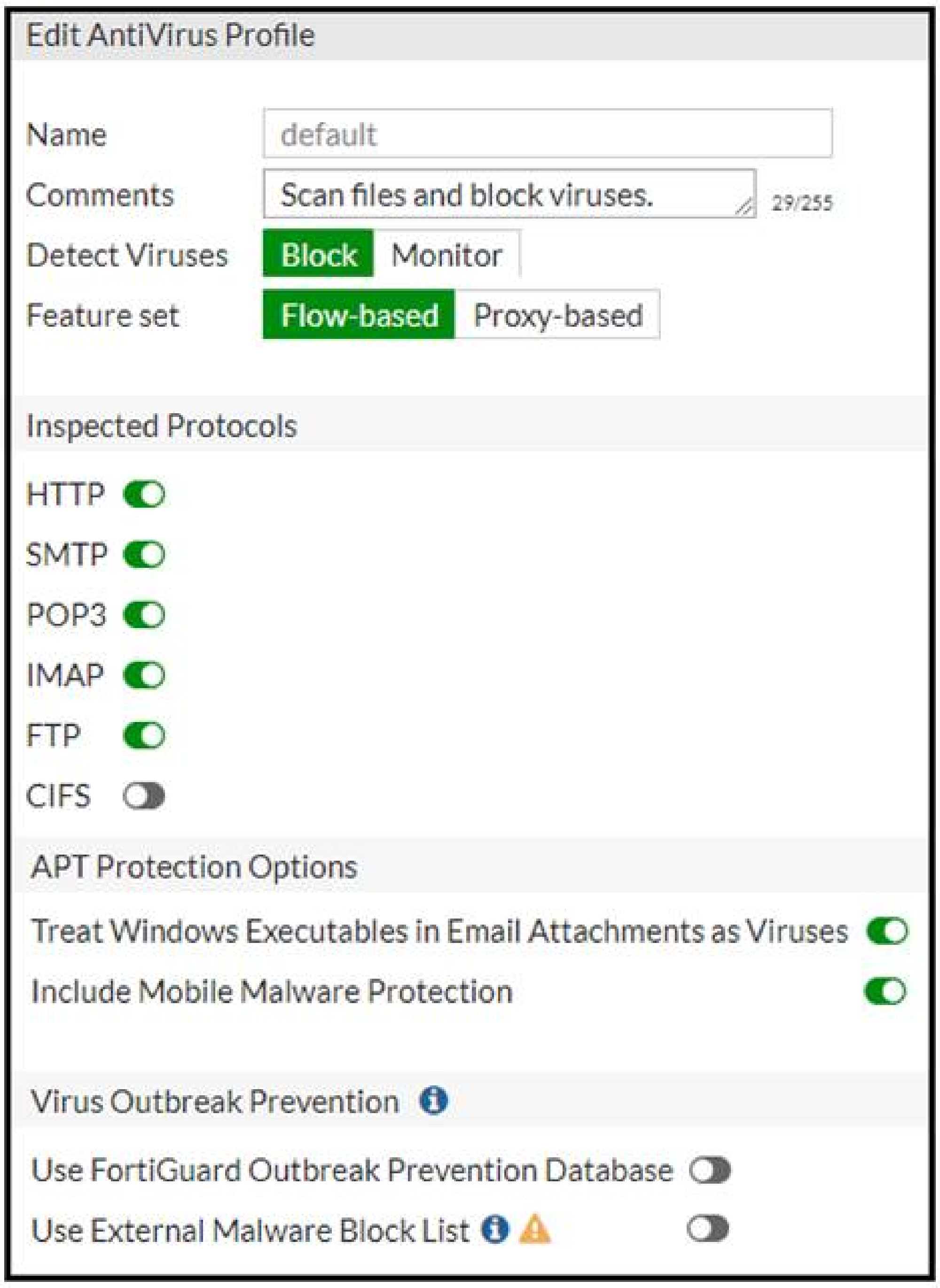
DNS Filter ○

Application Control ○

IPS ○

SSL Inspection ⚠ SSL deep-inspection

Decrypted Traffic Mirror ○



Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Detect Viruses: [✓ Block] Monitor

Feature set: [✓ Flow-based] Proxy-based

Inspected Protocols

HTTP ●

SMTP ●

POP3 ●

IMAP ●

FTP ●

CIFS ○

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses ●

Include Mobile Malware Protection ●

Virus Outbreak Prevention

Use FortiGuard Outbreak Prevention Database ○

Use External Malware Block List ○

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The firewall policy performs the full content inspection on the file.
B. The flow-based inspection is used, which resets the last packet to the user.
C. The volume of traffic being inspected is too high for this model of FortiGate.
D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: B

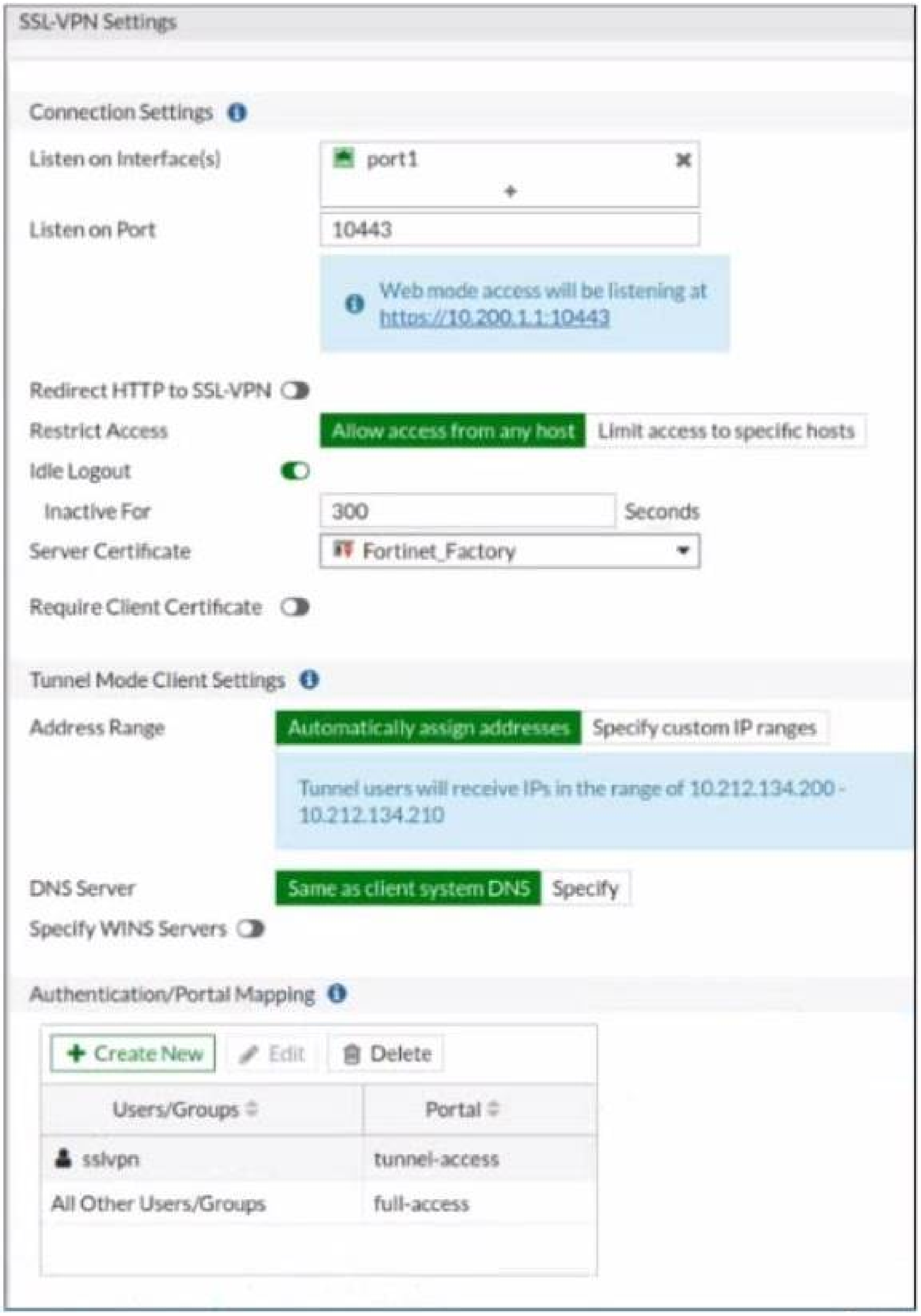
Explanation:
· "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
· When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

NEW QUESTION 12
Which three statements explain a flow-based antivirus profile? (Choose three.)

A. Flow-based inspection uses a hybrid of the scanning modes available in proxy-based inspection.
B. If a virus is detected, the last packet is delivered to the client.
C. The IPS engine handles the process as a standalone.
D. FortiGate buffers the whole file but transmits to the client at the same time.
E. Flow-based inspection optimizes performance compared to proxy-based inspection.

Answer: ADE

NEW QUESTION 15
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

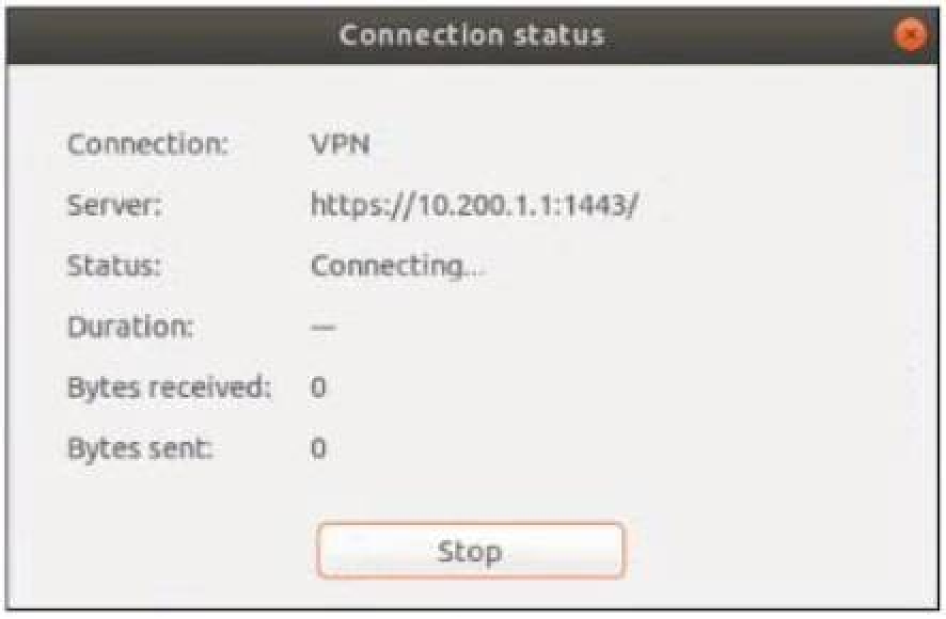
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210

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 status

Connection: VPN

Server: https://10.200.1.1:1443/

Status: Connecting...

Duration: —

Bytes received: 0

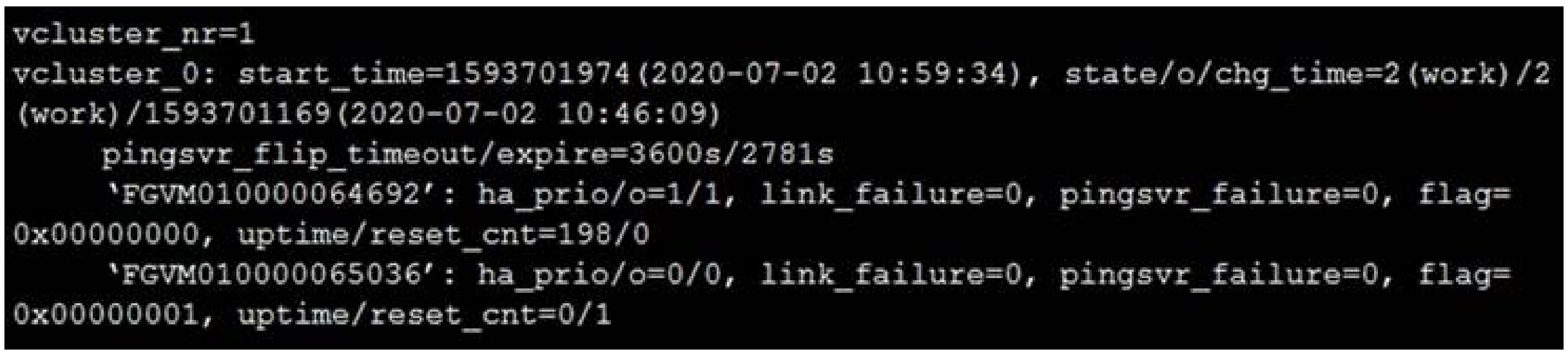
Bytes sent: 0

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

Answer: A

NEW QUESTION 18
Refer to the exhibit.



```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
     pingsvr_flip_timeout/expire=3600s/2781s
     'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
     'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.
B. FortiGate devices are not in sync because one device is down.
C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
D. FortiGate SN FGVM010000064692 has the higher HA priority.

Answer: AD

Explanation:
* 1. Override is disable by default - OK
* 2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary" The QUESTION NO: here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide. https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab

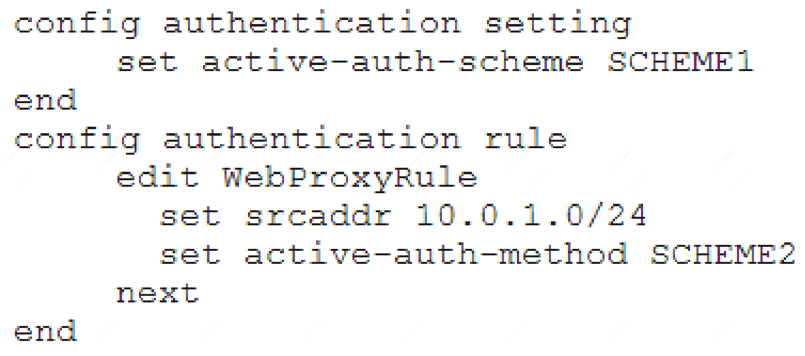
NEW QUESTION 21
Which two types of traffic are managed only by the management VDOM? (Choose two.)

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

Answer: AD

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.73): "What about traffic originating from FortiGate? Some system daemons, such as NTP and FortiGuard updates, generate traffic coming from FortiGate. Traffic coming from FortiGate to those global services originates from the management VDOM. One, and only one, of the VDOMs on a FortiGate device is assigned the role of the management VDOM. It is important to note that the management VDOM designation is solely for traffic originated by FortiGate, such as FortiGuard updates, and has no effect on traffic passing through FortiGate."

NEW QUESTION 25
Examine this FortiGate configuration:



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

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

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

Answer: D

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

NEW QUESTION 26
Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

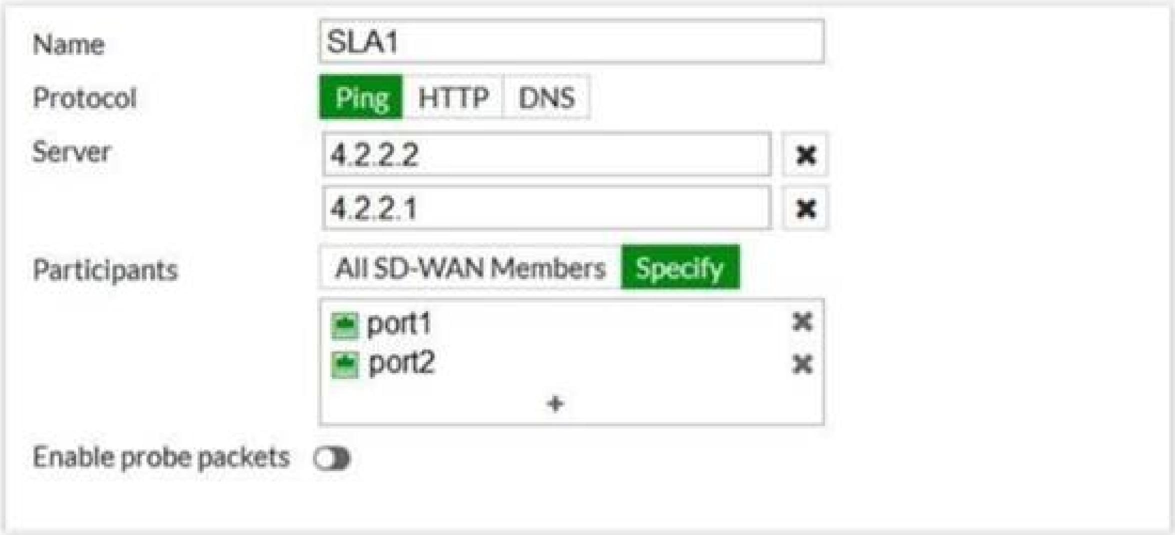
A. Source IP
B. Spillover
C. Volume
D. Session

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing

NEW QUESTION 30

Refer to the exhibit.



Name: SLA1

Protocol: Ping HTTP DNS

Server: 4.2.2.2
4.2.2.1

Participants: All SD-WAN Members Specify
port1
port2

Enable probe packets ○

An administrator has configured a performance SLA on FortiGate, which failed to generate any traffic. Why is FortiGate not sending probes to 4.2.2.2 and 4.2.2.1 servers? (Choose two.)

A. The Detection Mode setting is not set to Passive.
B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
C. The configured participants are not SD-WAN members.
D. The Enable probe packets setting is not enabled.

Answer: BD

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. 168.3.0/24
B. 192. 168.2.0/24
C. 192. 168. 1.0/24
D. 192. 168.0.0/8

Answer: B

NEW QUESTION 38

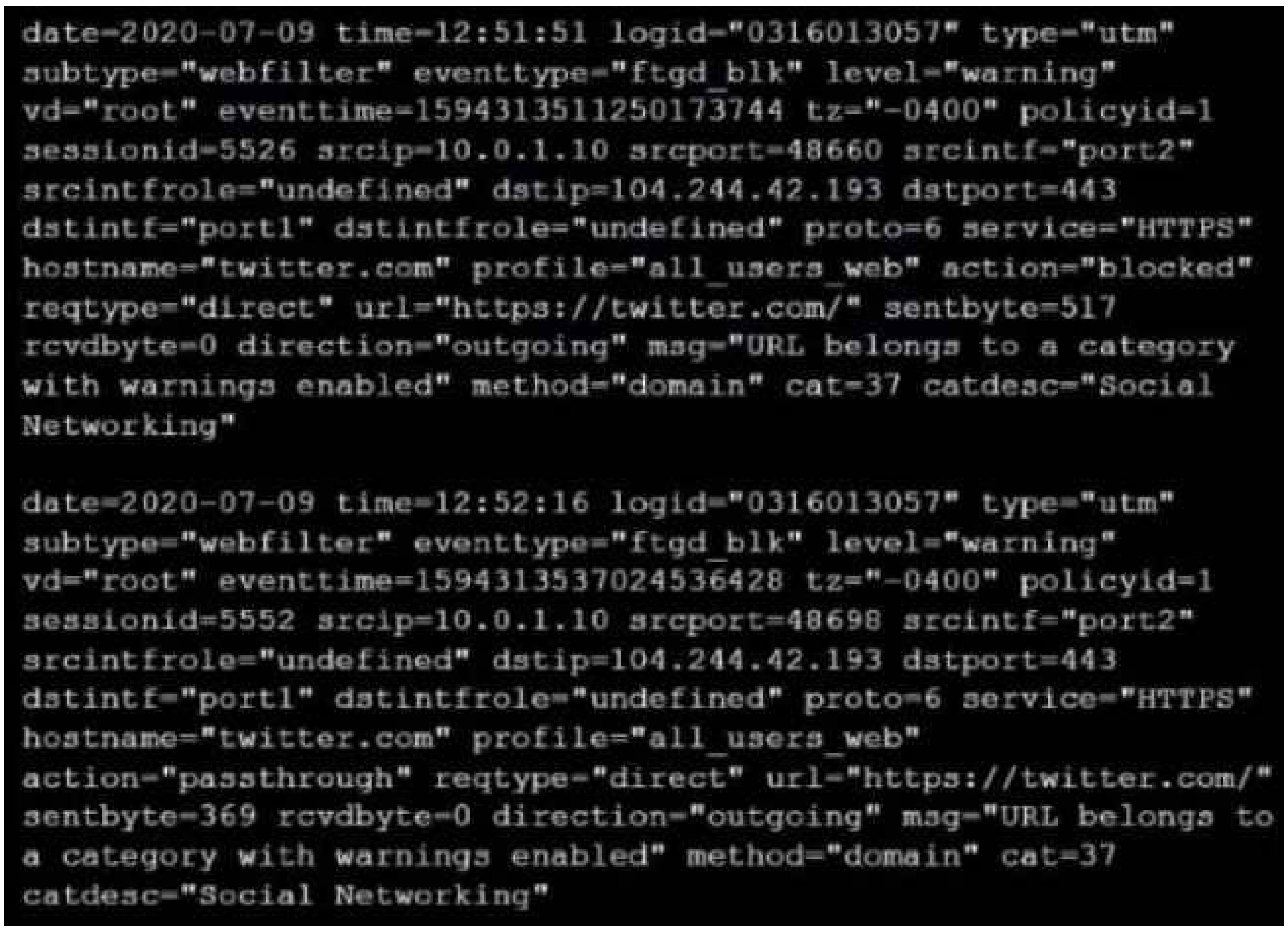
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache
B. FortiSIEM
C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Answer: BCE

NEW QUESTION 39

Refer to the web filter raw logs.



```
date=2020-07-09 time=12:51:51 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313511250173744 tz="-0400" policyid=1
sessionid=5526 srcip=10.0.1.10 srcport=48660 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web" action="blocked"
reqtype="direct" url="https://twitter.com/" sentbyte=517
rcvdbyte=0 direction="outgoing" msg="URL belongs to a category
with warnings enabled" method="domain" cat=37 catdesc="Social
Networking"

date=2020-07-09 time=12:52:16 logid="0316013057" type="utm"
subtype="webfilter" eventtype="ftgd_blk" level="warning"
vd="root" eventtime=1594313537024536428 tz="-0400" policyid=1
sessionid=5552 srcip=10.0.1.10 srcport=48698 srcintf="port2"
srcintfrole="undefined" dstip=104.244.42.193 dstport=443
dstintf="port1" dstintfrole="undefined" proto=6 service="HTTPS"
hostname="twitter.com" profile="all_users_web"
action="passthrough" reqtype="direct" url="https://twitter.com/"
sentbyte=369 rcvdbyte=0 direction="outgoing" msg="URL belongs to
a category with warnings enabled" method="domain" cat=37
catdesc="Social Networking"
```

Based on the raw logs shown in the exhibit, which statement is correct?

A. Social networking web filter category is configured with the action set to authenticate.
B. The action on firewall policy ID 1 is set to warning.
C. Access to the social networking web filter category was explicitly blocked to all users.
D. The name of the firewall policy is all_users_web.

Answer: A

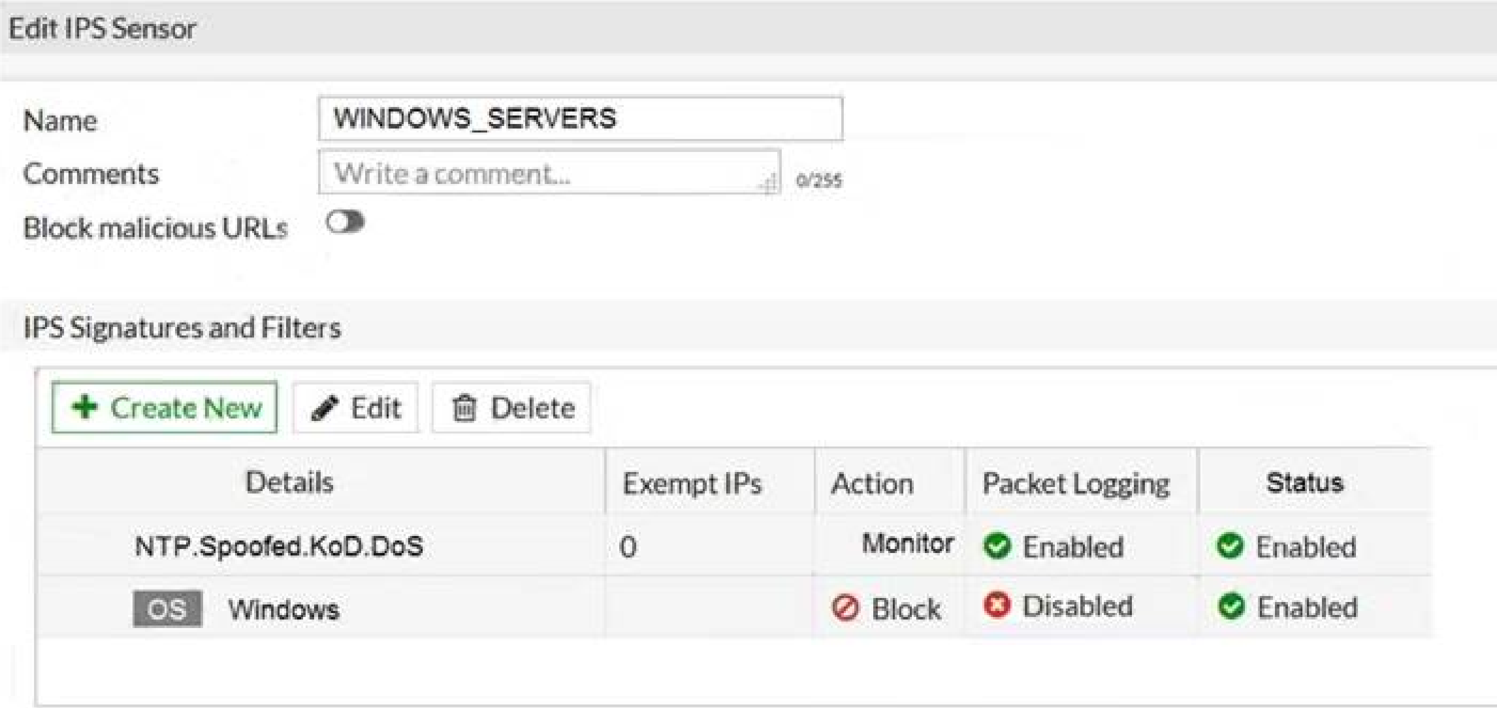
NEW QUESTION 40
When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

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

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.67): "When creating firewall objects or policies, a universally unique identifier (UUID) attribute is added so that logs can record these UUIDs and improve functionality when integrating with FortiManager or FortiAnalyzer."

NEW QUESTION 44
Refer to the exhibit.



Edit IPS Sensor

Name: WINDOWS_SERVERS
Comments: Write a comment... 0/255
Block malicious URLs: ○

IPS Signatures and Filters

Details	Exempt IPs	Action	Packet Logging	Status
NTP.Spoofed.KoD.DoS	0	Monitor	✓ Enabled	✓ Enabled
OS Windows		⊘ Block	✗ Disabled	✓ Enabled

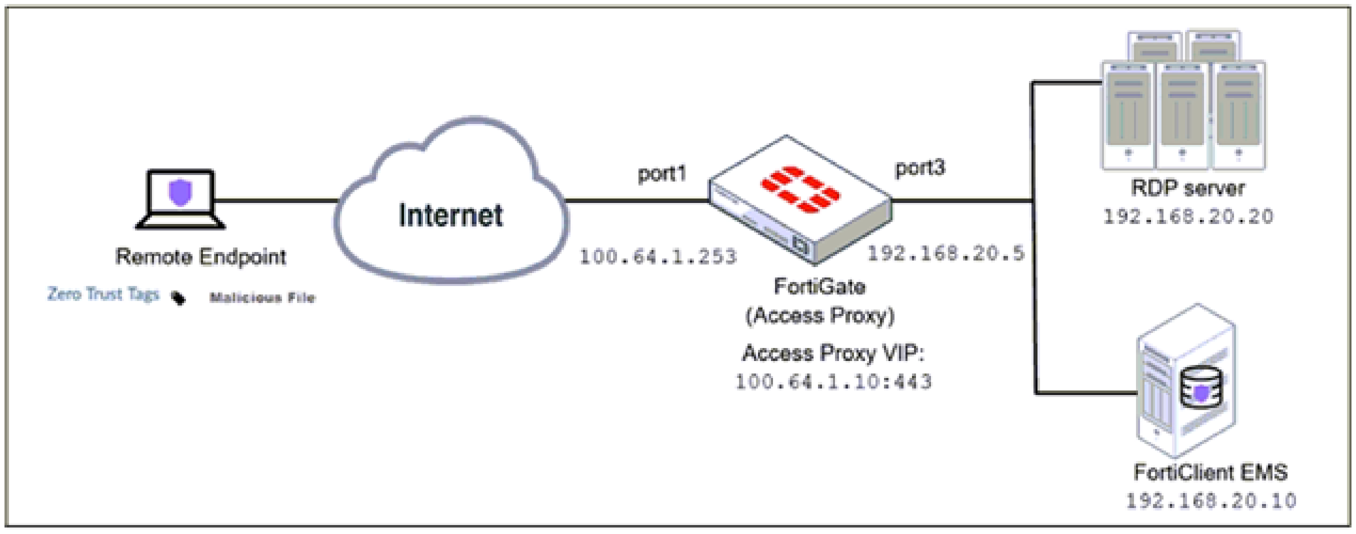
The exhibit shows the IPS sensor configuration.
If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.

C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 49
Refer to the exhibit.



Based on the ZTNA tag, the security posture of the remote endpoint has changed. What will happen to endpoint active ZTNA sessions?

A. They will be re-evaluated to match the endpoint policy.
B. They will be re-evaluated to match the firewall policy.
C. They will be re-evaluated to match the ZTNA policy.
D. They will be re-evaluated to match the security policy.

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-zt FortiGate Infrastructure 7.2 Study Guide (p.182): "Endpoint posture changes trigger active ZTNA proxy
sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy."

NEW QUESTION 51
Which feature in the Security Fabric takes one or more actions based on event triggers?

A. Fabric Connectors
B. Automation Stitches
C. Security Rating
D. Logical Topology

Answer: B

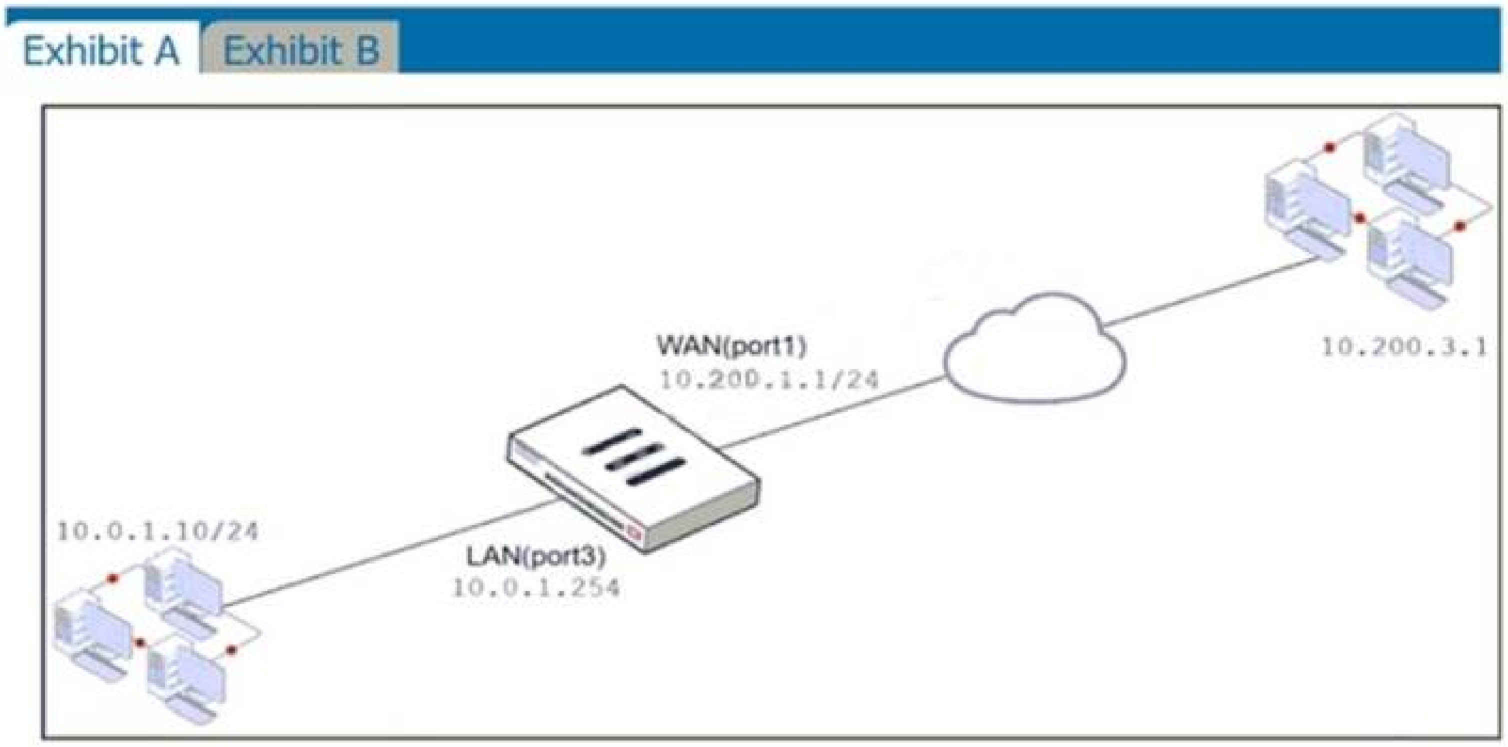
NEW QUESTION 53
Which statement describes a characteristic of automation stitches?

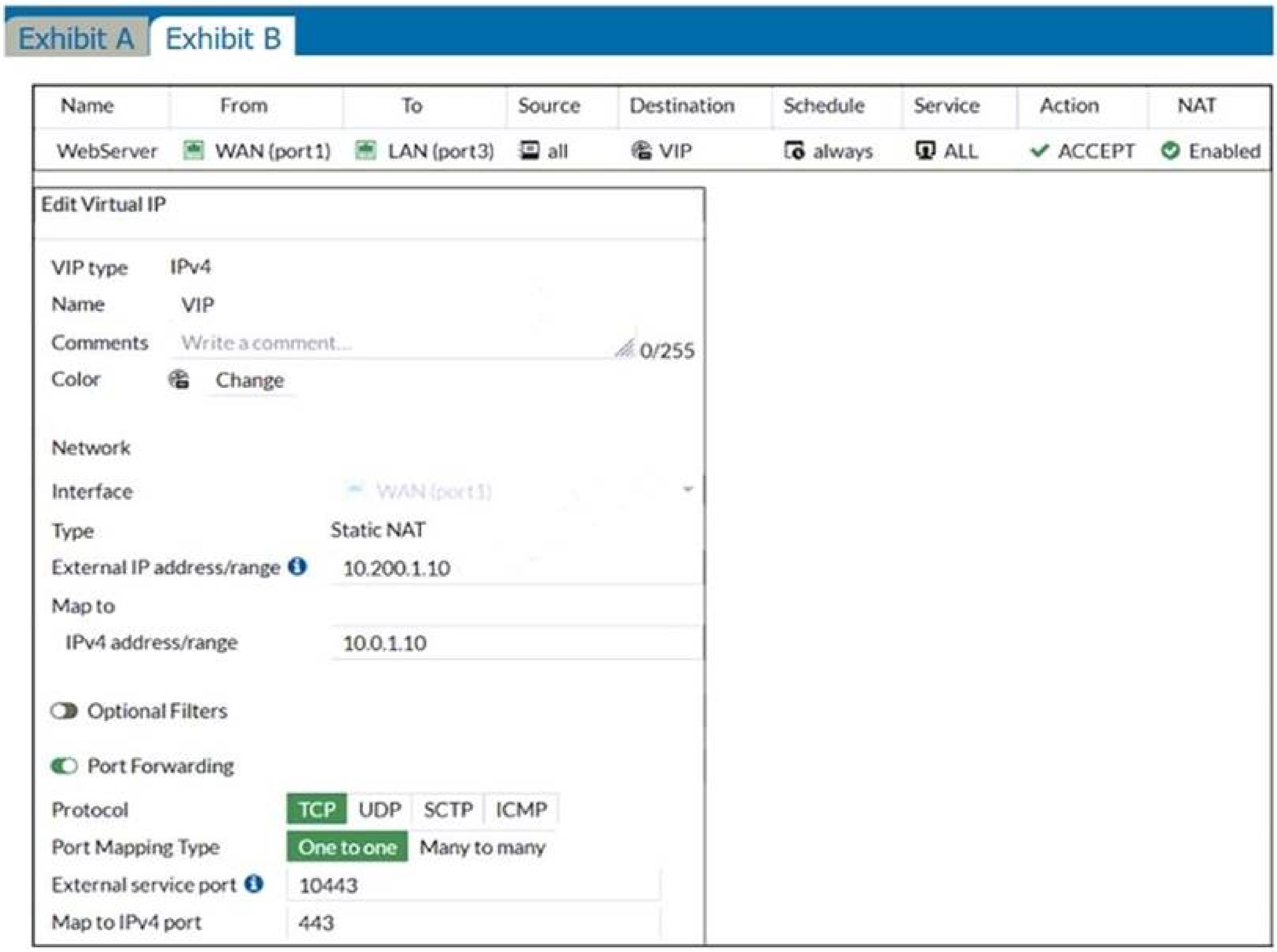
A. They can have one or more triggers.
B. They can be run only on devices in the Security Fabric.
C. They can run multiple actions simultaneously.
D. They can be created on any device in the fabric.

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches

NEW QUESTION 57
Examine the exhibit, which contains a virtual IP and firewall policy configuration.





Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	✓ ACCEPT	✓ Enabled

Edit Virtual IP

VIP type	IPv4
Name	VIP
Comments	Write a comment... 0/255
Color	Change

Network

Interface	WAN (port1)
Type	Static NAT
External IP address/range	10.200.1.10
Map to	
IPv4 address/range	10.0.1.10

○ Optional Filters

● Port Forwarding

Protocol	TCP UDP SCTP ICMP
Port Mapping Type	One to one Many to many
External service port	10443
Map to IPv4 port	443

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 66 of 108
C. 10.200. 1. 1
D. 10.0. 1.254

Answer: A

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

NEW QUESTION 62
What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

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

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=12069
FortiGate Infrastructure 7.2 Study Guide (p.264): "...then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable Auto-negotiate. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away." "Another benefit of enabling Auto-negotiate is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable Autokey Keep Alive and keep Auto-negotiate disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable Auto-negotiate, Autokey Keep Alive is implicitly enabled."

NEW QUESTION 67
Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

A. Warning
B. Exempt
C. Allow
D. Learn

Answer: AC

NEW QUESTION 71
Which of the following statements about central NAT are true? (Choose two.)

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

Answer: AB

NEW QUESTION 76
An administrator needs to increase network bandwidth and provide redundancy.
What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface
B. Software Switch interface
C. Aggregate interface
D. Redundant interface

Answer: C

Explanation:
An aggregate interface is a logical interface that combines two or more physical interfaces into one virtual interface1. An aggregate interface can increase network bandwidth and provide redundancy by distributing traffic across multiple physical interfaces using a load balancing algorithm1. An aggregate interface can also support link aggregation control protocol (LACP) to negotiate the link aggregation settings with the connected device1.

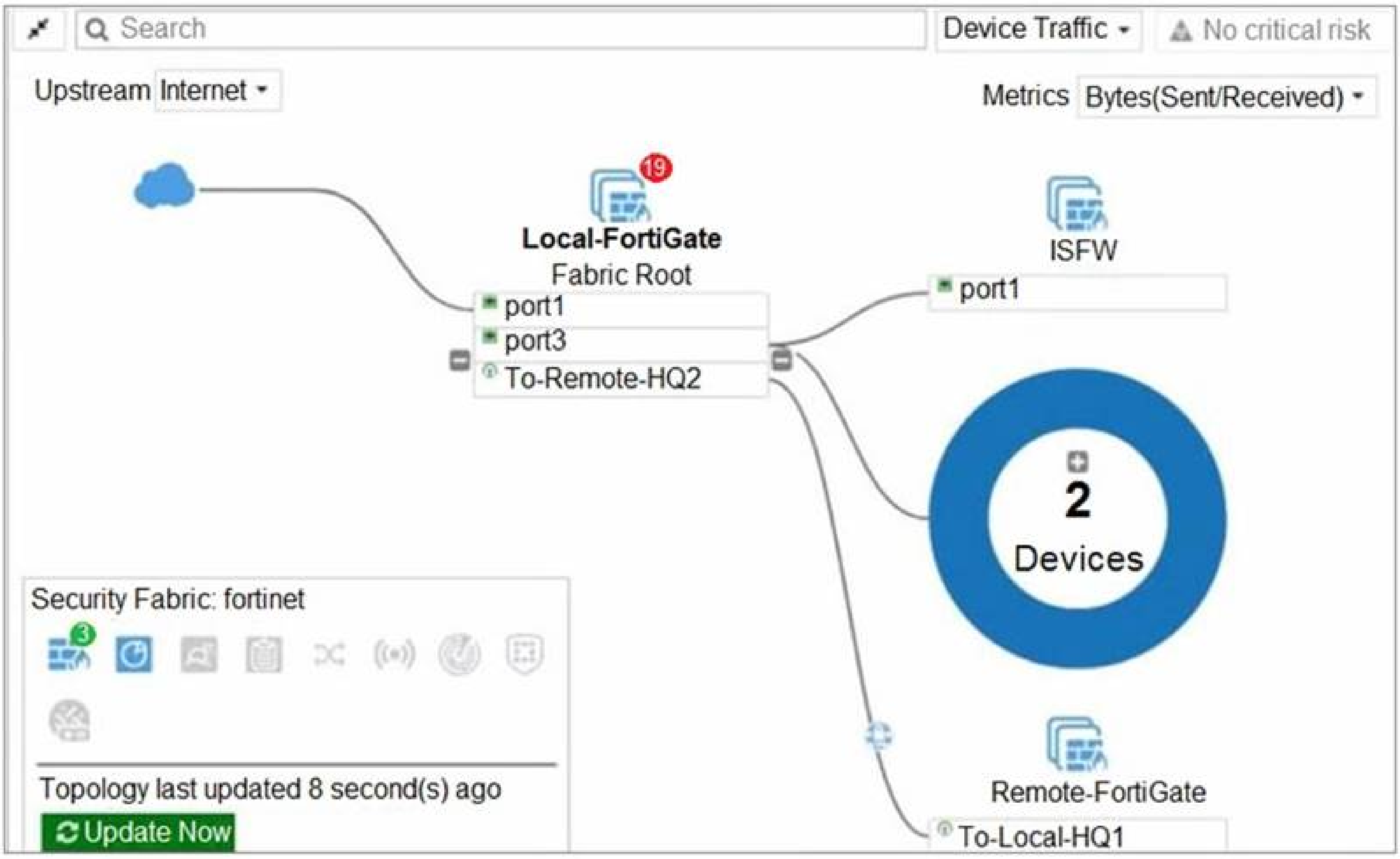
NEW QUESTION 80
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

A. get system status
B. get system performance status
C. diagnose sys top
D. get system arp

Answer: D

Explanation:
"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

NEW QUESTION 82
Refer to the exhibit.



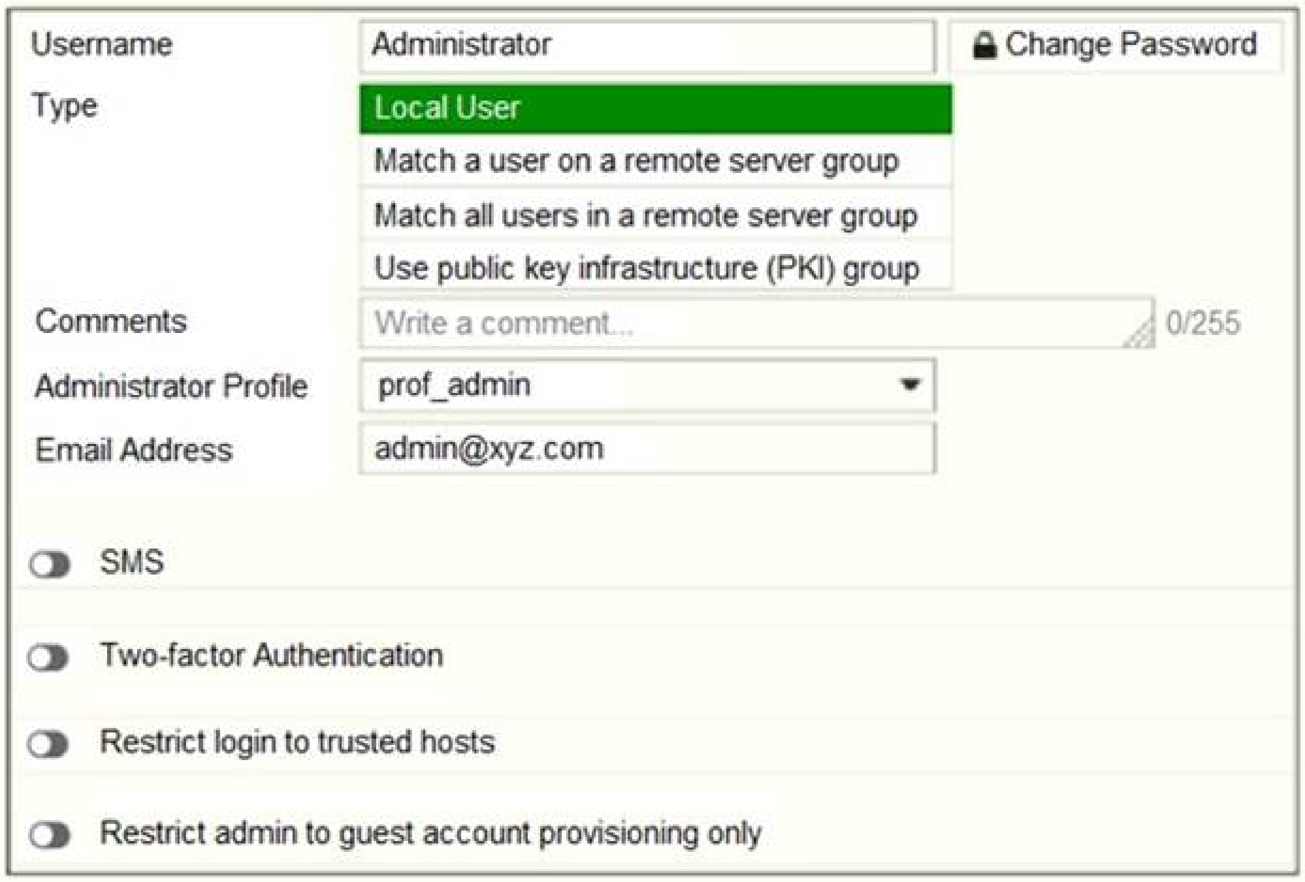
Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

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

Answer: CD

Explanation:
References: https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology

NEW QUESTION 87
Refer to the exhibit.



Username	Administrator	Change Password
Type	Local User Match a user on a remote server group Match all users in a remote server group Use public key infrastructure (PKI) group	
Comments	Write a comment...	0/255
Administrator Profile	prof_admin	
Email Address	admin@xyz.com	

○ SMS

○ Two-factor Authentication

○ Restrict login to trusted hosts

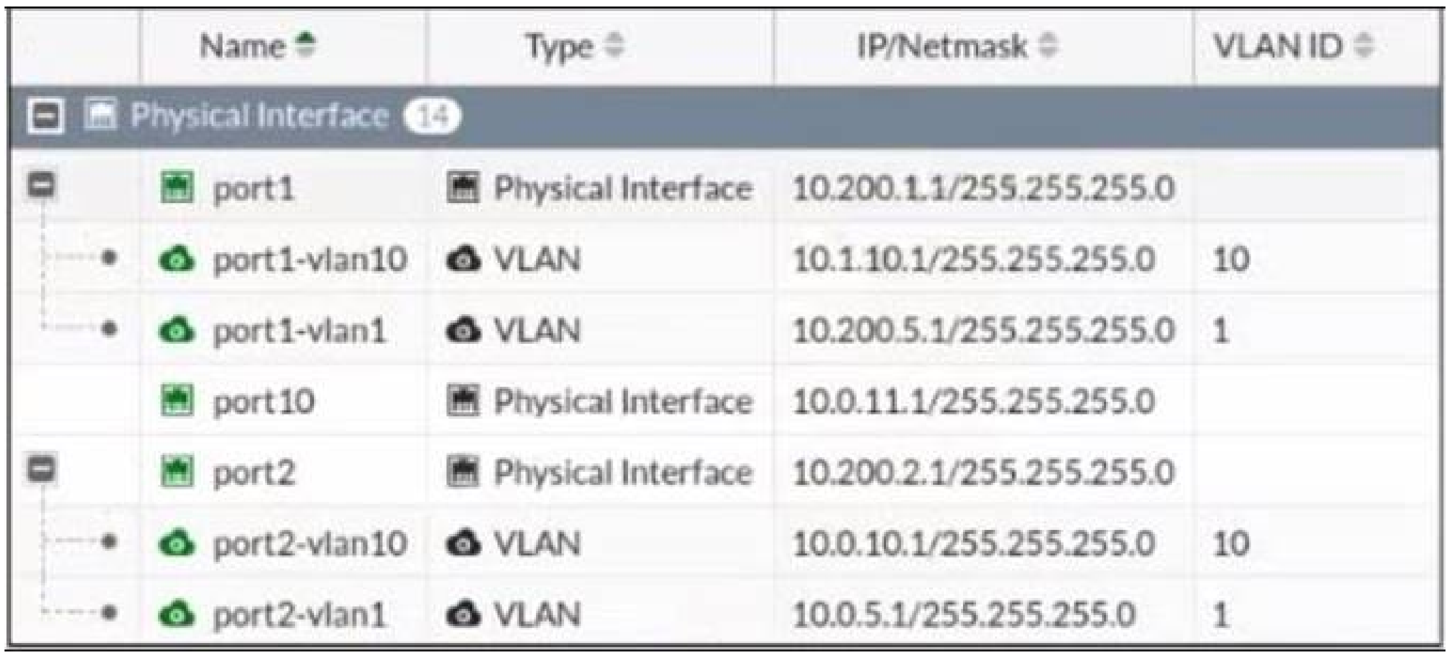
○ Restrict admin to guest account provisioning only

The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

A. Change password
B. Enable restrict access to trusted hosts
C. Change Administrator profile
D. Enable two-factor authentication

Answer: C

NEW QUESTION 88
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. Traffic between port2 and port2-vlan1 is allowed by default.
B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
C. port1 is a native VLAN.
D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Answer: CD

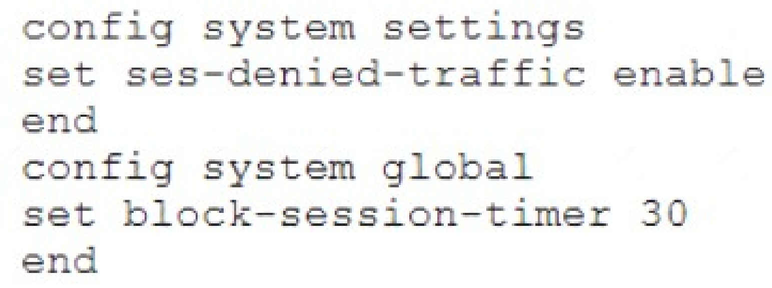
Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

NEW QUESTION 93
Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.
B. It is available only on a proxy-based firewall policy.
C. It inspects video files hosted on file sharing services.
D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer: B

NEW QUESTION 95
An administrator has configured the following settings:



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

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

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

Answer: CD

Explanation:
ses-denied-traffic
Enable/disable including denied session in the session table. https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/20620/config-system-settings block-session-timer
Duration in seconds for blocked sessions . integer
Minimum value: 1 Maximum value: 300
30
https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/1620/config-system-global

NEW QUESTION 96
Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.
B. AH does not support perfect forward secrecy.
C. AH provides data integrity bur no encryption.
D. AH provides strong data integrity but weak encryption.

Answer: C

NEW QUESTION 97

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

A. hard-timeout
B. auth-on-demand
C. soft-timeout
D. new-session
E. Idle-timeout

Answer: ADE

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

NEW QUESTION 99

......