

Fortinet.FCP_FGT_AD-7.6.v2026-04-06.q79

Exam Code:	FCP_FGT_AD-7.6
Exam Name:	FCP - FortiGate 7.6 Administrator
Certification Provider:	Fortinet
Free Question Number:	79
Version:	v2026-04-06
# of views:	175
# of Questions views:	790
https://www.exam-tests.com/FCP_FGT_AD-7.6-exam/Fortinet.FCP_FGT_AD-7.6.v2026-04-06.q79.html	

NEW QUESTION: 1

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

- A. Connected monitored ports > Priority > HA uptime > FortiGate serial number
- B. Connected monitored ports > Priority > System uptime > FortiGate serial number
- C. Connected monitored ports > HA uptime > Priority > FortiGate serial number
- D. Connected monitored ports > System uptime > Priority > FortiGate serial number

Answer: A (LEAVE A REPLY)

When HA override is enabled, FortiGate uses the following election order: number of connected monitored ports, then device priority, followed by HA uptime, and finally FortiGate serial number as a tiebreaker.

NEW QUESTION: 2

Refer to the exhibit.



The NOC team connects to the FortiGate GUI with the NOC_Access admin profile. They request that their GUI sessions do not disconnect too early during inactivity. What must the administrator configure to answer this specific request from the NOC team?

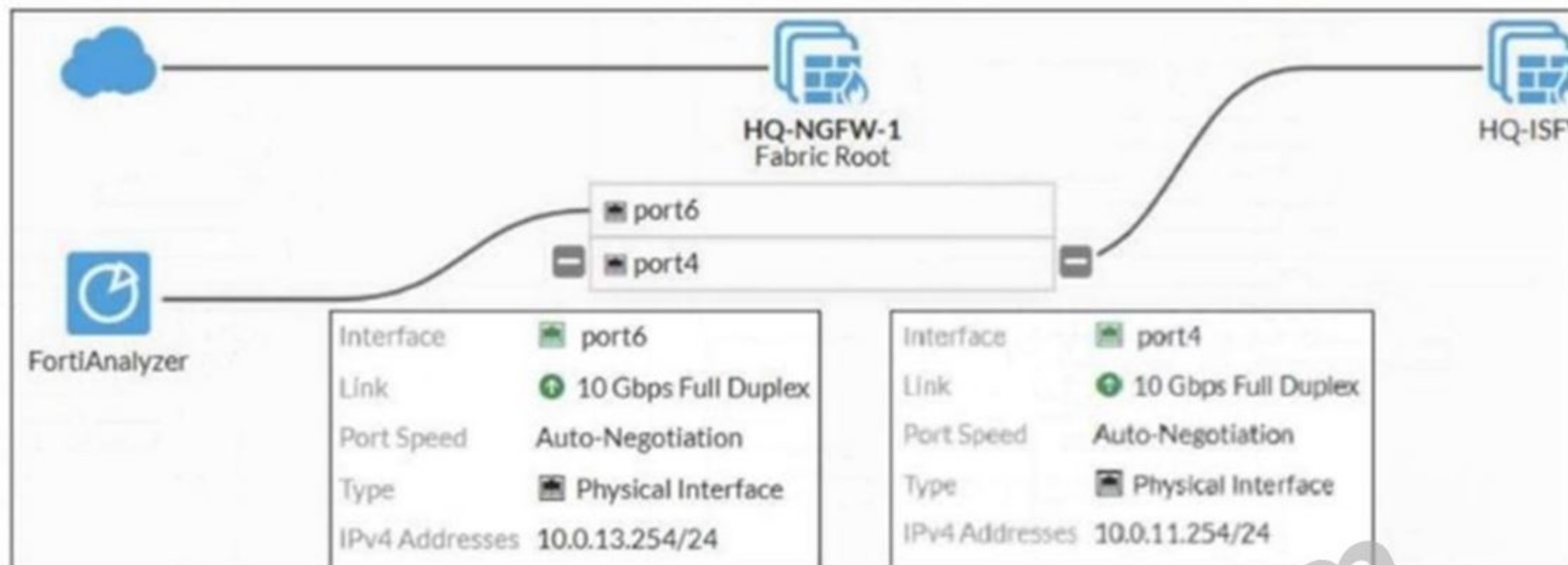
- A. Move NOC_Access to the top of the list to ensure all profile settings take effect.
- B. Increase the offline value of the Override Idle Timeout parameter in the NOC_Access admin profile.
- C. Ensure that all NOC_Access users are assigned the super_admin role to guarantee access
- D. Increase the admintimeout value under config system accprofile NOC_Access.

Answer: (SHOW ANSWER)

The admintimeout setting in the admin access profile controls the inactivity timeout for GUI sessions. Increasing this value will extend the session duration before automatic disconnection.

NEW QUESTION: 3

Refer to the exhibits. An administrator wants to add HQ-ISFW-2 in the Security Fabric. HQ-ISFW-2 is in the same subnet as HQ-ISFW. After configuring the Security Fabric settings on HQ-ISFW-2, the status stays Pending.



Security Fabric settings on HQ-ISFW-2

Security Fabric Settings

Security Fabric role: ☐ Standalone ☐ Serve as Fabric Root ☒ Join Existing Fabric

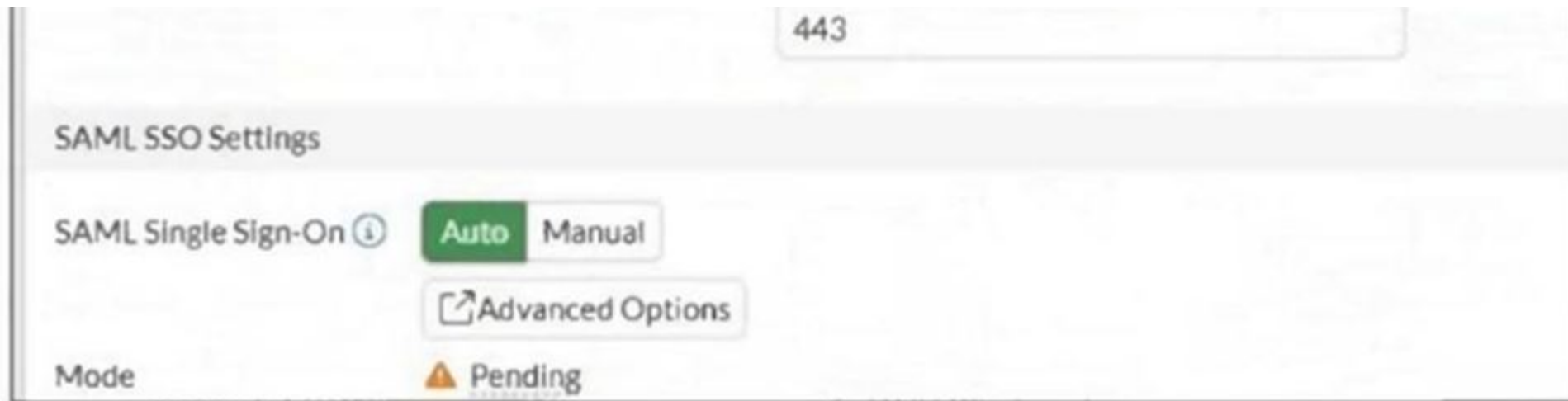
Allow other Security Fabric devices to join: ☐ ☒ port6

Upstream FortiGate IP/FQDN: 10.0.13.254

Allow downstream device REST API access: ☐ ☒

Management IP/FQDN: ☐ Use WAN IP ☒ Specify 10.0.11.250

Management port: ☐ Use Admin Port ☒ Specify



What can be the two possible reasons? (Choose two.)

- A. Upstream FortiGate IP must be set to 10.0.11.254.
- B. SAML Single Sign-On must be set to Manual.
- C. HQ-ISFW-2 must be authorized on HQ-ISFW.
- D. Management IP must be set to 10.0.13.254.

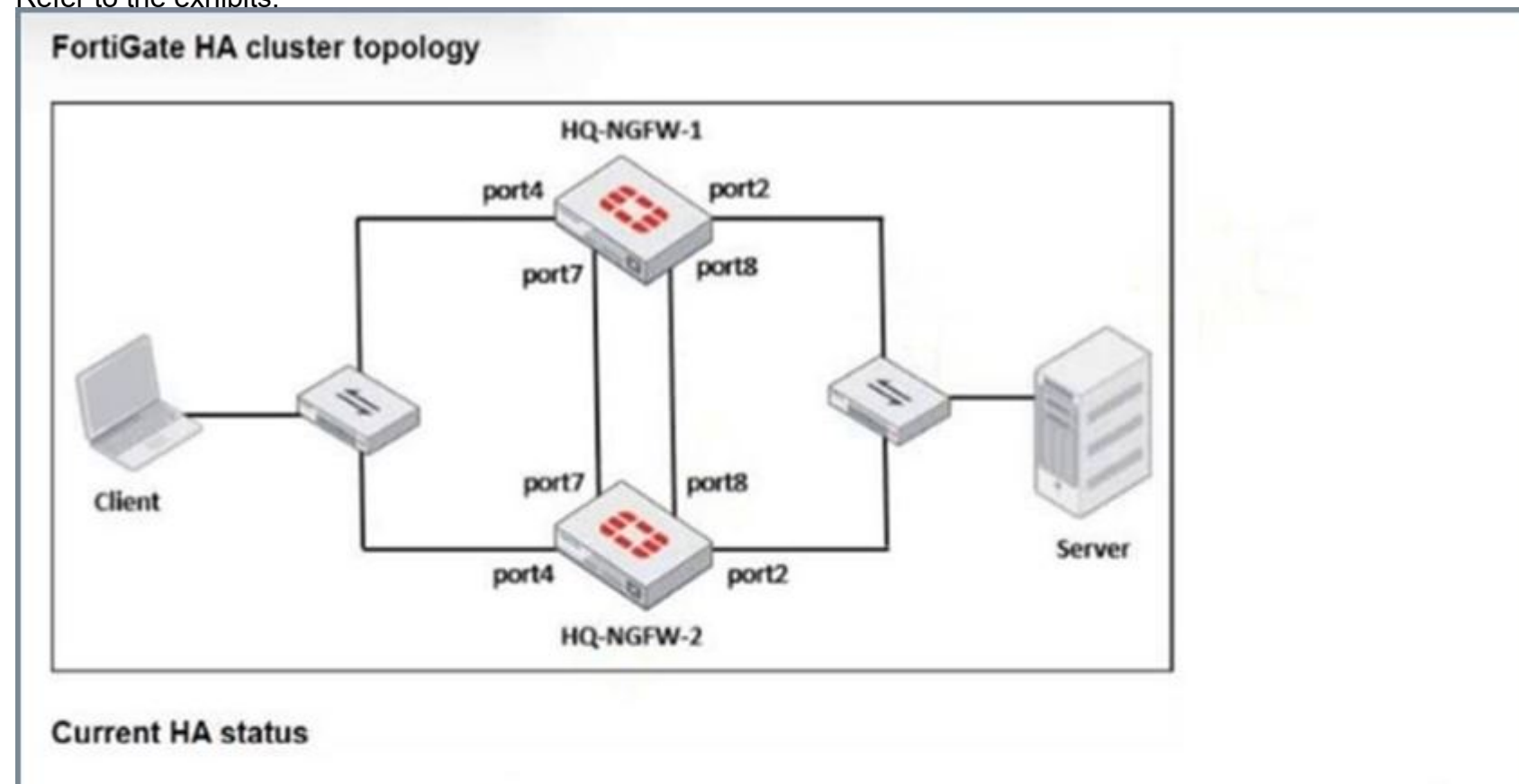
Answer: A,C ([LEAVE A REPLY](#))

The Upstream FortiGate IP should match the IP address of the Fabric Root interface, which is 10.0.11.254, not 10.0.13.254.

The new device (HQ-ISFW-2) must be authorized on the Fabric Root (HQ-ISFW) before it can join the Security Fabric, otherwise the status remains pending.

NEW QUESTION: 4

Refer to the exhibits.



```

HQ-NGFW-1 # get system ha status
...
Configuration Status:
  FGVM02TM24013423(updated 0 seconds ago): in-sync
  FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
  FGVM02TM24013501(updated 4 seconds ago): in-sync
  FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1      , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2      , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, HA operating index = 1

```

New FortiGate HA configuration

```

HQ-NGFW-1
# config system ha
  set group-id 5
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port7" 50 "port8" 60
  set session-pick enable
  set override disable
  set priority 90
  set monitor "port3"

HQ-NGFW-2
# config system ha
  set group-id 5
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port7" 50 "port8" 60
  set session-pick enable
  set override enable
  set priority 110
  set monitor "port3"

```

Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibit.

What would be the expected outcome in the HA cluster?

- A. HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.
- B. HQ-NGFW-2 will take over as the primary because it has the override enable setting and higher priority than HQ-NGFW-1.
- C. HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority.
- D. The HA cluster will become out of sync because the override setting must match on all HA members.

Answer: ([SHOW ANSWER](#))

With override enabled on HQ-NGFW-2 and its higher priority (110 vs. 90), HQ-NGFW-2 will become the primary device, preempting HQ-NGFW-1 despite the current primary status.

NEW QUESTION: 5

What are two features of the NGFW profile-based mode? (Choose two.)

- A. NGFW profile-based mode can only be applied globally and not on individual VDOMs.
- B. NGFW profile-based mode must require the use of central source NAT policy.
- C. NGFW profile-based mode policies support both flow inspection and proxy inspection.
- D. NGFW profile-based mode supports applying applications and web filtering profiles in a firewall policy.

Answer: C,D ([LEAVE A REPLY](#))

NGFW (Next Generation Firewall) profile-based mode in FortiGate allows policies to use both flow- based and proxy-based inspection modes, providing flexibility depending on security and performance requirements. Additionally, profile-based mode supports applying applications and web filtering profiles directly in a firewall policy, allowing granular control over the traffic.

NEW QUESTION: 6

Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, and the firewall policies, VIP, and IP pool configurations on the FortiGate device.

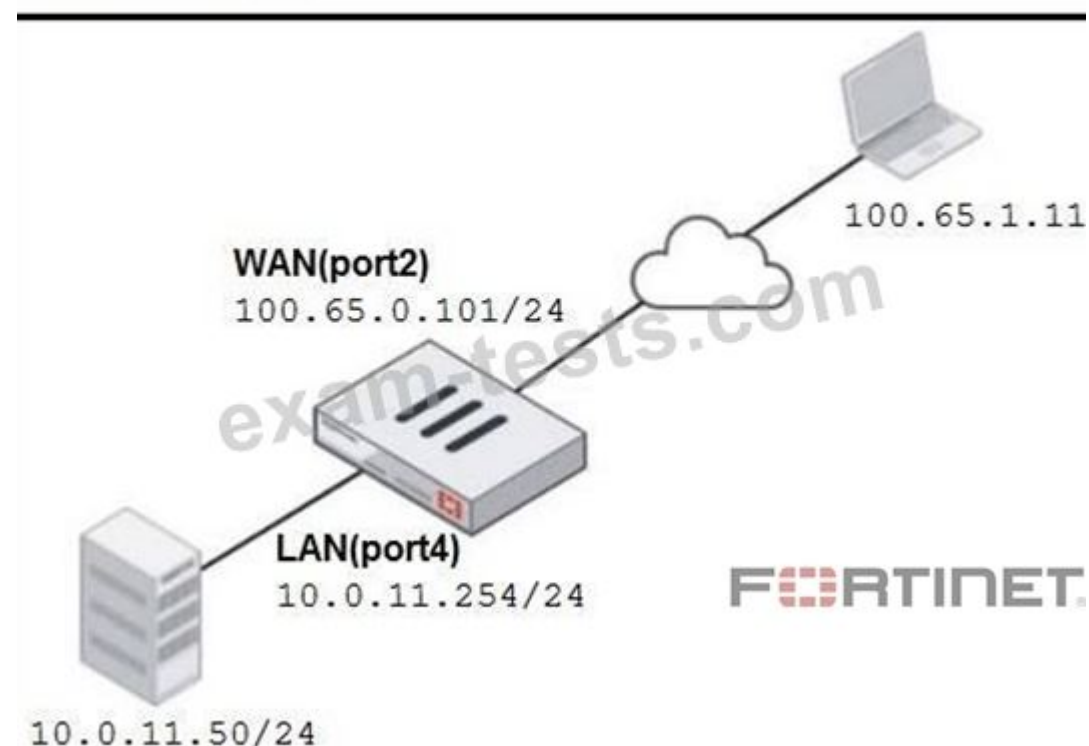
The WAN (port2) interface has the IP address 100.65.0.101/24.

The LAN (port4) interface has the IP address 10.0.11.254/24.

The first firewall policy has NAT enabled using the IP pool. The second firewall policy is configured with a VIP as the destination address.

Which IP address will be used to source NAT (SNAT) the internet traffic coming from a workstation with the IP address 10.0.11.50?

Network diagram



Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☐	Internet(1)	LAN(port4)	WAN(port2)	all	all	always	ALL	✓ ACCEPT	IP Pool	✓ NAT
☐	WebServer(2)	WAN(port2)	LAN(port4)	all	VIP	always	ALL	✓ ACCEPT		✗ Disabled

VIP configuration

Edit Virtual IP

Name

Comments 0/255

Color 

Network

Interface 

Type

External IP address/range 

Map to

IPv4 address/range

☐ Optional Filters

☒ Port Forwarding

Protocol

Port Mapping Type

External service port 

Map to IPv4 port

NAT IP pool configuration

Edit Dynamic IP Pool

Name

IP Pool

Comments

Write a comment... 0/255

Type

Overload

External IP Range ⓘ

100.65.0.102–100.65.0.102

NAT64

☐

ARP Reply

☒

- A. 100.65.0.101
- B. 100.65.0.200
- C. 100.65.0.102
- D. 10.0.11.254

Answer: (SHOW ANSWER)

Traffic from the workstation 10.0.11.50 going to the internet matches the Internet(1) policy (LAN → WAN) which has NAT enabled and is configured to use the IP Pool. The IP pool specifies the external address 100.65.0.102. FortiGate will perform source NAT (SNAT) on the outbound traffic, translating the source IP of the workstation to 100.65.0.102.

NEW QUESTION: 7

Refer to the exhibit.

```
config system global
    set av-failopen one-shot
end
config ips global
    set fail-open enable
end
```

Based on this partial configuration, what are the two possible outcomes when FortiGate enters conserve mode? (Choose two.)

- A. Administrators cannot change the configuration.
- B. FortiGate skips quarantine actions.
- C. Administrators must restart FortiGate to allow new session.
- D. FortiGate drops new sessions requiring inspection.

Answer: B,D (LEAVE A REPLY)

In fail-open mode, FortiGate skips quarantine actions to maintain traffic flow despite IPS or antivirus failures.

FortiGate drops new sessions that require inspection when in conserve mode and fail-open is enabled, to protect the network from potentially harmful traffic.

NEW QUESTION: 8

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

- A.** Security Rating Insights are available only in the Security Rating page.
- B.** The Security Posture category provides PCI compliance results.
- C.** The root FortiGate provides executive summaries of all the FortiGate devices in the Security Fabric.
- D.** A license is required to obtain an executive summary in the Security Rating section.

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 9

What are two features of FortiGate FSSO agentless polling mode? (Choose two.)

- A.** FortiGate directs the collector agent to use a remote LDAP server.
- B.** FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C.** FortiGate does not support workstation check.
- D.** FortiGate uses the AD server as the collector agent.

Answer: B,D ([LEAVE A REPLY](#))

FortiGate uses the SMB protocol to read the event viewer logs from the DCs → In agentless polling mode, FortiGate connects directly to the AD domain controllers using SMB to collect logon events.

FortiGate uses the AD server as the collector agent → There is no external FSSO collector; instead, the FortiGate itself polls the AD servers, effectively treating them as the source of logon information.

NEW QUESTION: 10

A network administrator is configuring an IPsec VPN tunnel for a sales employee travelling abroad.

Which IPsec Wizard template must the administrator apply?

- A.** Hub-and-Spoke
- B.** Site to Site
- C.** Remote Access
- D.** Dial up User

Answer: C ([LEAVE A REPLY](#))

The Remote Access IPsec Wizard template is used for individual users connecting from remote locations, such as traveling employees. This template configures FortiGate to act as an IPsec VPN server, allowing remote clients (like FortiClient) to securely connect and access internal network resources while abroad.

NEW QUESTION: 11

Which two statements describe characteristics of automation stitches? (Choose two.)

- A.** Actions involve only devices included in the Security Fabric.
- B.** An automation stitch can have multiple triggers.
- C.** Multiple actions can run in parallel.
- D.** Triggers can involve external connectors.

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 12

Automation stitches can execute multiple actions concurrently (in parallel). Triggers for automation stitches can come from external connectors beyond just Fortinet devices. Refer to the exhibits.

Categories

☒ Mixed • All Categories

- ☒ Business (157, 6)
- ☒ Collaboration (266, 13)
- ☒ Game (83)
- ☒ Mobile (3)
- ☒ Operational Technology
- ☒ Proxy (189)
- ☒ Social Media (113, 29)
- ☒ Update (48)
- ☒ VoIP (23)
- ☒ Unknown Applications
- ☒ Cloud/IT (72, 12)
- ☒ Email (76, 11)
- ☒ General Interest (254, 15)
- ☒ Network Services (30)
- ☒ P2P (55)
- ☒ Remote Access (96)
- ☒ Storage/Backup (150, 20)
- ☒ Video/Audio (148, 17)
- ☒ Web Client (24)

☒ Network Protocol Enforcement

Application and Filter Overrides

+ Create New ✓ Edit ✕ Delete				
Priority	Details		Type	Action
1	WARN	Excessive-Bandwidth	Filter	☒ Block
2	WARN	Google	Filter	☒ Monitor

Firewall policy



Edit Policy

Firewall / Network Options

Inspection Mode ☒ Flow-based ☐ Proxy-based

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options ☒ default

Security Profiles

AntiVirus ☐

Web Filter ☐

DNS Filter ☐

Application Control ☒ ☒ default

IPS ☐

File Filter ☐

SSL Inspection ☒ certificate-Inspection

Logging Options

Log Allowed Traffic ☒ Security Events ☒ All Sessions

You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.

You cannot access any of the Google applications, but you are able to access www.fortinet.com.

What would you do to resolve this issue?

- A. Change the Inspection mode to Proxy-based.
- B. Move up Google in the Application and Filter Overrides section to set its priority to 1.
- C. Set SSL inspection to deep-content-inspection.
- D. Add *Google*.com to the URL category in the security profile.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 13

An administrator notices that some users are unable to establish SSL VPN connections, while others can connect without any issues.

What should the administrator check first?

- A. Ensure that the affected users are using the correct port number.
- B. Ensure that user traffic is hitting the firewall policy.
- C. Ensure that forced tunneling is enabled to reroute all traffic through the SSL VPN
- D. Ensure that the HTTPS service is enabled on SSL VPN tunnel interface

Answer: A ([LEAVE A REPLY](#))

The key part of the question is some users can connect and some cannot, which strongly suggests a client-side connection issue rather than a firewall-policy issue (policy only applies after the tunnel is established).

For SSL-VPN, the first thing to check when users fail to connect is whether they are using the correct connection settings (especially the port).

NEW QUESTION: 14

When configuring firewall policies which of the following is true regarding the policy ID?

- A. It is mandatory to provide a policy ID while creating a firewall policy regardless of GUI or CLI.
- B. A firewall policy ID identifies the order of policy execution in firewall policies.
- C. You can create a policy in CLI with policy ID 0.
- D. A policy ID cannot be edited once a policy is created.

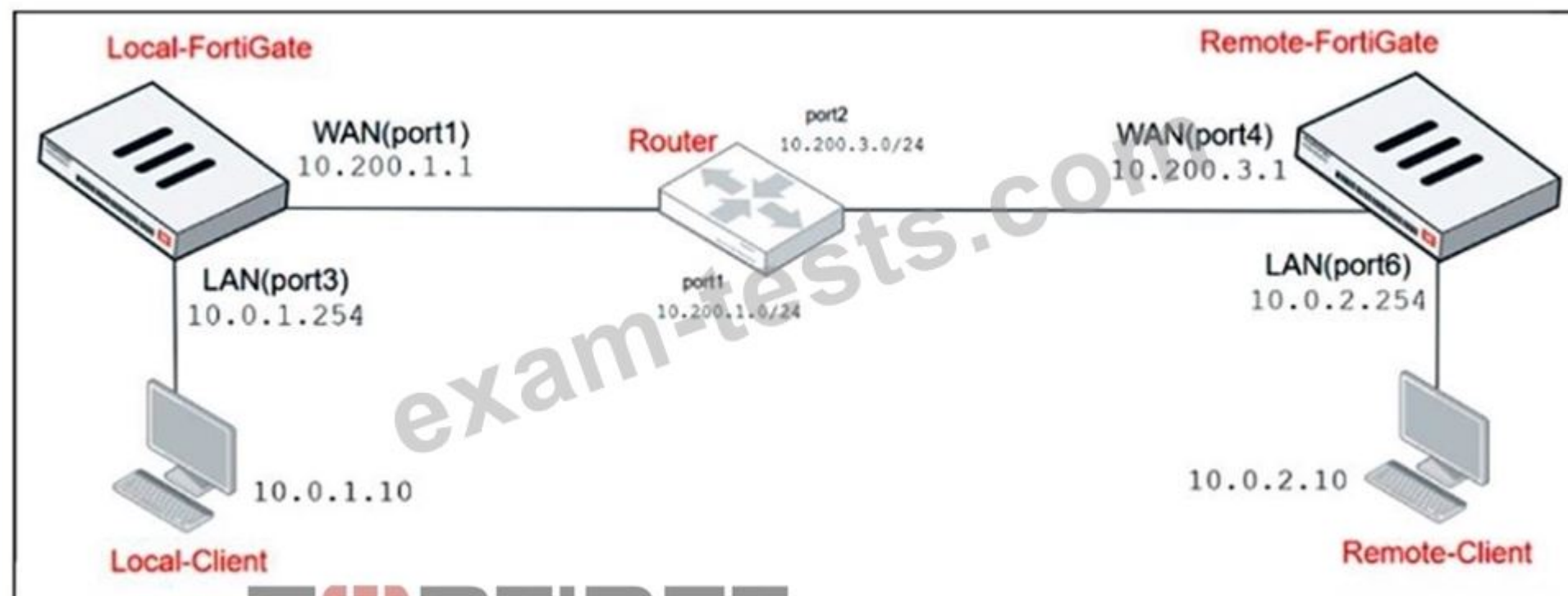
Answer: D ([LEAVE A REPLY](#))

Once a firewall policy is created, its policy ID is fixed and cannot be changed; this ID uniquely identifies the policy within the FortiGate configuration.

NEW QUESTION: 15

Refer to the exhibits.

Network diagram



NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	10.200.1.49 - 10.200.1.49	Overload	Enabled
SNAT-Remote	10.200.1.149 - 10.200.1.149	Overload	Enabled
SNAT-Remote1	10.200.1.99 - 10.200.1.99	Overload	Enabled

Firewall policy

ID	Name	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port3) → WAN (port1)								
2	TCP traffic	all	REMOTE_FORTIGATE	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
6	PING traffic	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
7	IGMP traffic	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.

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.

Which IP address will be used to source NAT (SNAT) the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

- A. 10.200.1.1
- B. 10.200.1.149
- C. 10.200.1.99
- D. 10.200.1.49

Answer: (SHOW ANSWER)

All_TCP doesn't include ICMP. So you would match rule ID 2, in which uses IP Poop remote 1.

NEW QUESTION: 16

Refer to the exhibit, which shows a partial configuration from the remote authentication server.

Attribute	Value	Vendor	Actions
Fortinet-Group-Name	Training	Fortinet	 

Why does the FortiGate administrator need this configuration?

- A. To set up a RADIUS server Secret.
- B. To authenticate Any FortiGate user groups.
- C. To authenticate and match the Training OU on the RADIUS server.
- D. To authenticate only the Training user group.

Answer: D (LEAVE A REPLY)

The Fortinet-Group-Name attribute is used to restrict authentication to users who belong specifically to the "Training" user group on the RADIUS server.

Valid FCP_FGT_AD-7.6 Dumps shared by BraindumpsPass.com for Helping Passing FCP_FGT_AD-7.6 Exam! BraindumpsPass.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the BraindumpsPass.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com FCP_FGT_AD-7.6 dumps with Test Engine here: https://www.braindumpspass.com/Fortinet/FCP_FGT_AD-7.6-practice-exam-dumps.html (132 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

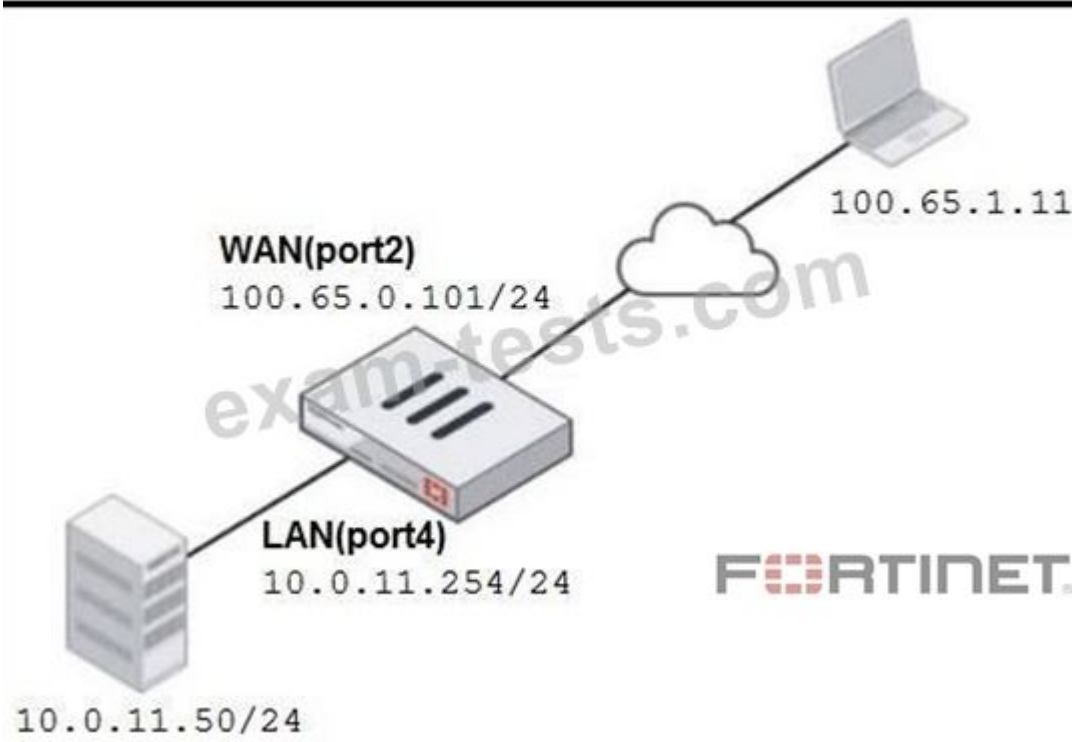
Refer to the exhibits. A diagram of a FortiGate device connected to the network VIP object and firewall policy configurations are shown.

The WAN (port2) interface has the IP address 100.65.0.101/24.

The LAN (port4) interface has the IP address 10.0.11.254/24.

If the host 100.65.1.111sends a TCP SYN packet on port 443 to 100.65.0.200, what will the source address, destination address, and destination port of the packet be at the time FortiGate forwards the packet to the destination?

Network diagram



VIP object configuration

Edit Virtual IP

Name

Comments 0/255

Color 

Network

Interface 

Type

External IP address/range 

Map to

IPv4 address/range

☐ Optional Filters

☒ Port Forwarding

Protocol

Port Mapping Type

External service port 

Map to IPv4 port

Firewall policies

	Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
☒	Internet(1)	 LAN(port4)	 WAN(port2)	 all	 all	 always	 ALL	✓ ACCEPT		 NAT
☐	Web_Server_Access(2)	 WAN(port2)	 LAN(port4)	 all	 VIP-WEB-SERVER	 always	 HTTPS	✓ ACCEPT		 Disabled

- A. 10.0.11.254, 10.0.15.50, and 4443, respectively
- B. 100.65.1.111, 10.0.11.50and 443, respectively
- C. 10.0.11.254, 100.65.0.200, and 443, respectively
- D. 100.65.1.111, 10.0.11.50, and 4443, respectively

Answer: (SHOW ANSWER)

The VIP object maps the external IP 100.65.0.200:443 to the internal server 10.0.11.50:4443.

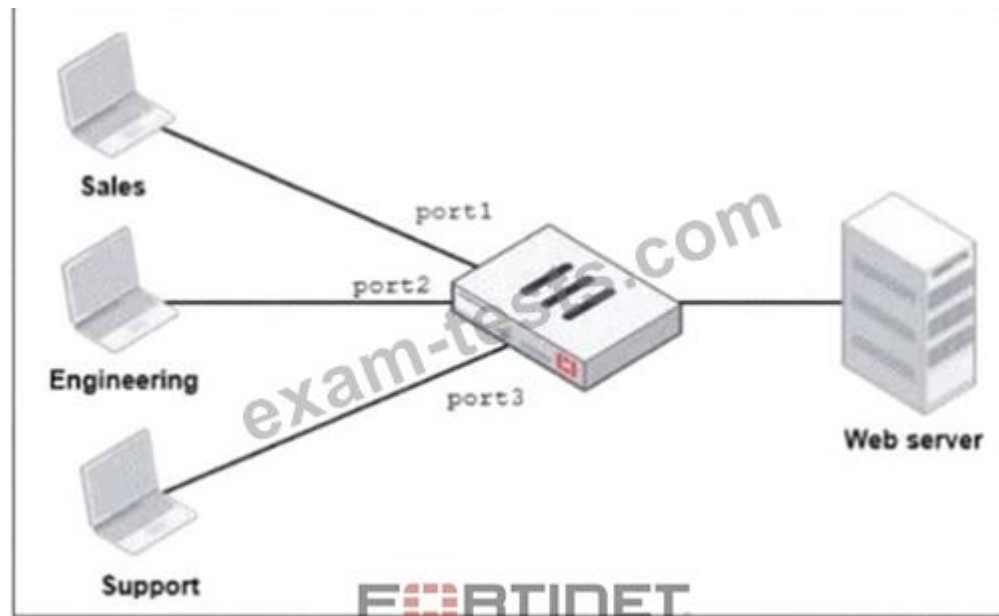
Since NAT is disabled on the firewall policy, the source IP is preserved.

So, when host 100.65.1.111 connects to 100.65.0.200:443:

- The source remains 100.65.1.111.
- The destination IP is translated to 10.0.11.50.
- The destination port is translated to 4443.

NEW QUESTION: 18

Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.

Which action must the administrator perform to consolidate the two policies into one?

- A.** Create an Aggregate interface that includes port1 and port2 to create a single firewall policy.
- B.** Select port1 and port2 subnets in a single firewall policy.
- C.** Replace port1 and port2 with the any interface in a single firewall policy.
- D.** Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy.

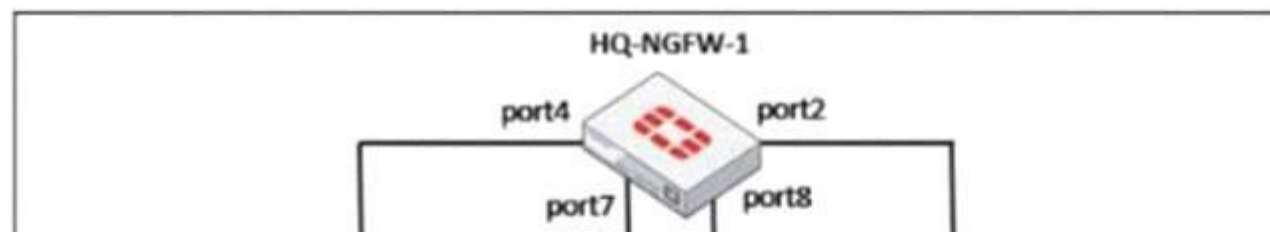
Answer: D (LEAVE A REPLY)

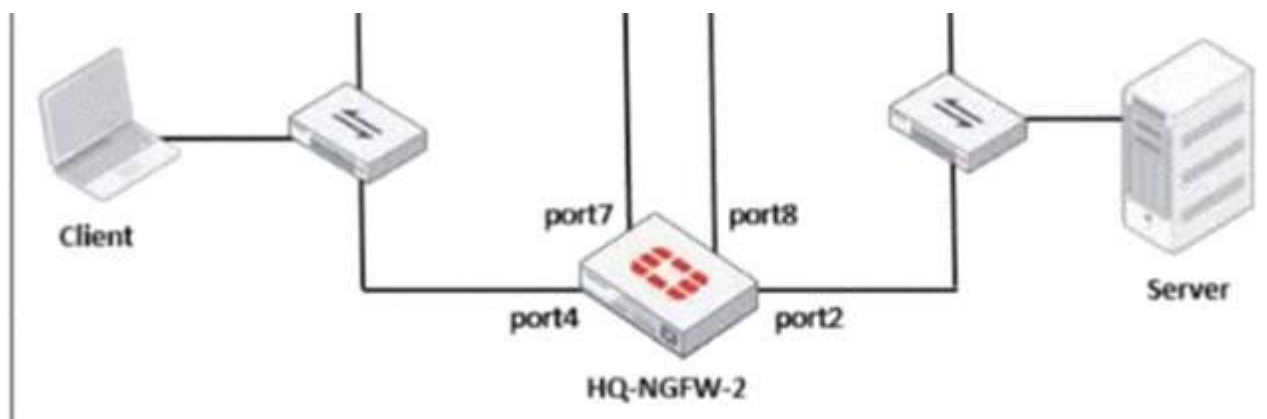
Enabling Multiple Interface Policies allows you to select multiple interfaces (like port1 and port2) in a single firewall policy, consolidating access rules for both Sales and Engineering to the web server.

NEW QUESTION: 19

Refer to the exhibits.

FortiGate HA cluster topology





Current HA status

```

HQ-NGFW-1 # get system ha status
...
Configuration Status:
  FGVM02TM24013423(updated 0 seconds ago): in-sync
  FGVM02TM24013423 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
  FGVM02TM24013501(updated 4 seconds ago): in-sync
  FGVM02TM24013501 chksum dump: e1 60 2e 42 b8 c1 c6 df 11 34 0c 21 80 79 a4 9f
...
number of member: 2
HQ-NGFW-1      , FGVM02TM24013423, HA cluster index = 1
HQ-NGFW-2      , FGVM02TM24013501, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM02TM24013423, HA operating index = 0
Secondary: FGVM02TM24013501, HA operating index = 1

```

New FortiGate HA configuration

```

HQ-NGFW-1
# config system ha
  set group-id 5
  set group-name "Fortinet"
  set mode a-p
  set password *
  set hbdev "port7" 50 "port8" 60
  set session-pick enable
  set override disable
  set priority 90
  set monitor "port3"

HQ-NGFW-2
# config system ha
  set group-id 5

```

```
set group-name "Fortinet"  
set mode a-p  
set password *  
set hbdev "port7" 50 "port8" 60  
set session-pick enable  
set override enable  
set priority 110  
set monitor "port3"
```

Based on the current HA status, an administrator updates the override and priority parameters on HQ-NGFW-1 and HQ-NGFW-2 as shown in the exhibit.

What would be the expected outcome in the HA cluster?

- A. HQ-NGFW-1 will synchronize the override disable setting with HQ-NGFW-2.
- B. HQ-NGFW-2 will take over as the primary because it has the override enable setting and higher priority than HQ-NGFW-1.
- C. HQ-NGFW-1 will remain the primary because HQ-NGFW-2 has lower priority.
- D. The HA cluster will become out of sync because the override setting must match on all HA members.

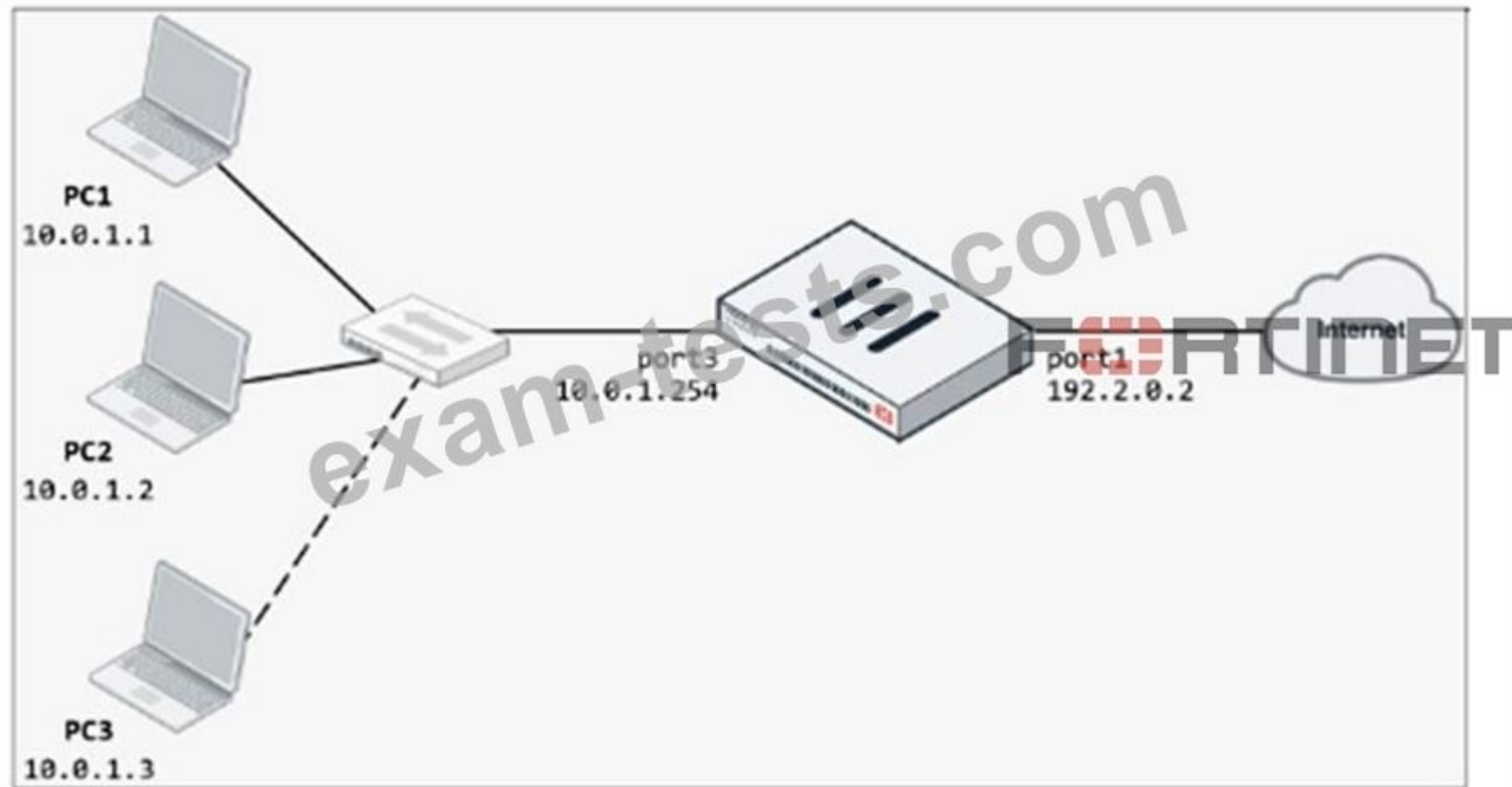
Answer: ([SHOW ANSWER](#))

With override enabled on HQ-NGFW-2 and its higher priority (110 vs. 90), HQ-NGFW-2 will become the primary device, preempting HQ-NGFW-1 despite the current primary status.

NEW QUESTION: 20

Refer to the exhibits.

Network diagram



Dynamic IP pool

Edit Dynamic IP Pool	
Name	internet-pool
Comments	Write a comment... 0/255
Type	One-to-One
External IP Range	192.2.0.10-192.2.0.11
ARP Reply	☒

Firewall policy

Edit Policy

Name	LAN-to-Internet
Incoming Interface	LAN (port3)
Outgoing Interface	WAN (port1)
Source	all
Destination	all
Schedule	always
Service	ALL
Action	☒ ACCEPT ☐ DENY
Inspection Mode	Flow-based ☒ Proxy-based
Firewall/Network Options	
NAT	☒
IP Pool Configuration	Use Outgoing Interface Address ☒ Use Dynamic IP Pool
	internet-pool
Preserve Source Port	☐
Protocol Options	☒ PROT default

The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.

Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.

Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

- A. In the IP pool configuration, set type to overload.
- B. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field.
- C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.
- D. In the IP pool configuration, set endip to 192.2.0.12.

Answer: (SHOW ANSWER)

With IP pool type set to One-to-One, only as many internal hosts as there are public IPs in the pool (192.2.0.10-192.2.0.11) can use NAT. Changing the type to overload allows all internal hosts (including PC3) to share the available public IPs, so PC3 can reach the internet.

Alternatively, keeping One-to-One but extending the pool to 192.2.0.10-192.2.0.12 adds another public IP, allowing a third internal host (PC3) to be mapped and gain internet access.

NEW QUESTION: 21

Refer to the exhibit. Why did FortiGate drop the packet?

```
id=65308 trace_id=6 func=print_pkt_detail line=5895 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:21637  
->10.200.1.254:2048) tun_id=0.0.0.0 from port3. type=8, code=0, id=21637, seq=2."  
id=65308 trace_id=6 func=init_ip_session_common line=6076 msg="allocate a new session-00025d45, tun_id=0.0.0.  
0"  
id=65308 trace_id=6 func=vf_ip_route_input_common line=2605 msg="find a route: flag=04000000 gw=10.200.1.254  
via port1"  
id=65308 trace_id=6 func=fw_forward_handler line=738 msg="Denied by forward policy check (policy 0)"
```

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

Answer: D (LEAVE A REPLY)

The debug trace output shows that the packet was "Denied by forward policy check (policy 0)." In FortiGate, policy ID 0 corresponds to the default implicit deny policy. This means that if a packet does not match any configured firewall policies, it is denied by the default implicit policy.

NEW QUESTION: 22

FortiGate web filter profile configuration

Edit Web Filter Profile

Name

Corporate

Comments

Write a comment...

0/255

Feature set

Flow-based

Proxy-based

☒ FortiGuard Category Based Filter

☒ Allow

☐ Monitor

☐ Block

☐ Warning

☐ Authenticate

Name	Action
☐ Bandwidth Consuming 6	
Freeware and Software Downloads	☒ Allow
File Sharing and Storage	☒ Allow
Streaming Media and Download	☒ Allow
Peer-to-peer File Sharing	☒ Allow
Internet Radio and TV	☒ Allow
Internet Telephony	☒ Allow
☐ Security Risk 6	
Malicious Websites	☐ Block

35% 21

The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.

An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.

What are two solutions for satisfying the requirement? (Choose two.)

- A.** Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.
- B.** Configure a web override rating for download.com and select Malicious Websites as the subcategory.
- C.** Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.
- D.** Set the Freeware and Software Downloads category Action to Warning.

Answer: (SHOW ANSWER)

Creating a static URL filter to block download.com specifically allows blocking that site without affecting the entire category.

Using a separate firewall policy with a Deny action for an FQDN address object matching download.com can also block the site while allowing others in the same category.

NEW QUESTION: 23

Which two statements are correct when FortiGate enters conserve mode? (Choose two.)

- A.** FortiGate continues to run critical security actions, such as quarantine.
- B.** FortiGate refuses to accept configuration changes.
- C.** FortiGate halts complete system operation and requires a reboot to regain available resources.
- D.** FortiGate continues to transmit packets without IPS inspection when the fail-open global setting in IPS is enabled.

Answer: B,D (LEAVE A REPLY)

In conserve mode, FortiGate restricts configuration changes to preserve system stability.

When IPS fail-open is enabled, FortiGate continues forwarding traffic without IPS inspection during resource constraints (conserve mode).

NEW QUESTION: 24

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 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 sent and reply packet of any new session.

Answer: A,C (LEAVE A REPLY)

The RPF (Reverse Path Forwarding) check is used to prevent IP spoofing attacks by verifying that the source IP address of a received packet is reachable through the same interface it arrived on. If not, the packet is dropped, ensuring traffic legitimacy.

The RPF check runs on the first sent packet of any new session to validate that the route to the source IP is consistent with the interface it's received on. This helps FortiGate detect spoofed or asymmetric routing scenarios early in the session establishment.

NEW QUESTION: 25

Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true?

(Choose two.)

- A.** If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
- B.** If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP.
- C.** If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.
- D.** If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance- mode.

Answer: A,D (LEAVE A REPLY)

When SD-WAN is disabled, FortiGate supports volume-based ECMP mode via the v4-ecmp- mode parameter.

When SD-WAN is enabled, the load balancing algorithm is controlled by the load-balance-mode parameter within the SD-WAN configuration.

NEW QUESTION: 26

Refer to the exhibits. You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits.

Which two factors can you observe from these configurations? (Choose two.)

Application sensor

Edit Application Sensor

Categories

 Mixed ▾ All Categories

-  ▾ Business (157,  6)
-  ▾ Collaboration (266,  13)
-  ▾ Game (83)
-  ▾ Mobile (3)
-  ▾ Operational Technology
-  ▾ Proxy (189)
-  ▾ Social Media (113,  29)
-  ▾ Update (48)
-  ▾ VoIP (23)
-  ▾ Unknown Applications
-  ▾ Cloud/IT (72,  12)
-  ▾ Email (76,  11)
-  ▾ General Interest (254,  15)
-  ▾ Network Service (338)
-  ▾ P2P (55)
-  ▾ Remote Access (96)
-  ▾ Storage/Backup (150,  20)
-  ▾ Video/Audio (148,  17)
-  ▾ Web Client (24)

☒ Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#)

[Edit](#)

[Delete](#)

Priority	Details	Type	Action
1	 Excessive-Bandwidth	Filter	 Block
2	 Google	Filter	 Monitor

2

Firewall policy

FORTINET
FORTINET®

Edit Policy

Firewall/Network Options

Inspection mode **Flow-based** Proxy-based

NAT ☒

IP pool configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve source port ☐

Protocol options **PROT** default ▼

Security Profiles

AntiVirus ☐

Web filter ☐

DNS filter ☐

Application control ☒ **APP** default ▼

IPS ☐

File filter ☐

SSL inspection ⚠ **SSL** deep-inspection ▼

Decrypted traffic mirror ☐

Logging Options



- A. YouTube search is allowed based on the Google Application and Filter override settings.
- B. YouTube access is blocked based on Excessive-Bandwidth Application and Filter override settings.
- C. Facebook access is allowed but you cannot play Facebook videos based on Video/Audio category filter settings.
- D. Facebook access is blocked based on the category filter settings.

Answer: ([SHOW ANSWER](#))

Facebook belongs to the Social Media application category, which is set to Block in the application sensor. Therefore, any Facebook application traffic is blocked by category.

The Excessive-Bandwidth behavior filter is configured as an override with priority 1 and action Block. YouTube streaming applications are tagged with the Excessive-Bandwidth behavior, so this override takes precedence over the Google (vendor) monitor rule and results in YouTube being blocked.

NEW QUESTION: 27

You have configured an application control profile, set peer-to-peer traffic to Block under the Categories tab, and applied it to the firewall policy. However, your peer-to-peer traffic on known ports is passing through the FortiGate without being blocked.

What FortiGate settings should you check to resolve this issue?

- A. FortiGuard category ratings
- B. Application and Filter Overrides
- C. Network Protocol Enforcement
- D. Replacement Messages for UDP-based Applications

Answer: ([SHOW ANSWER](#))

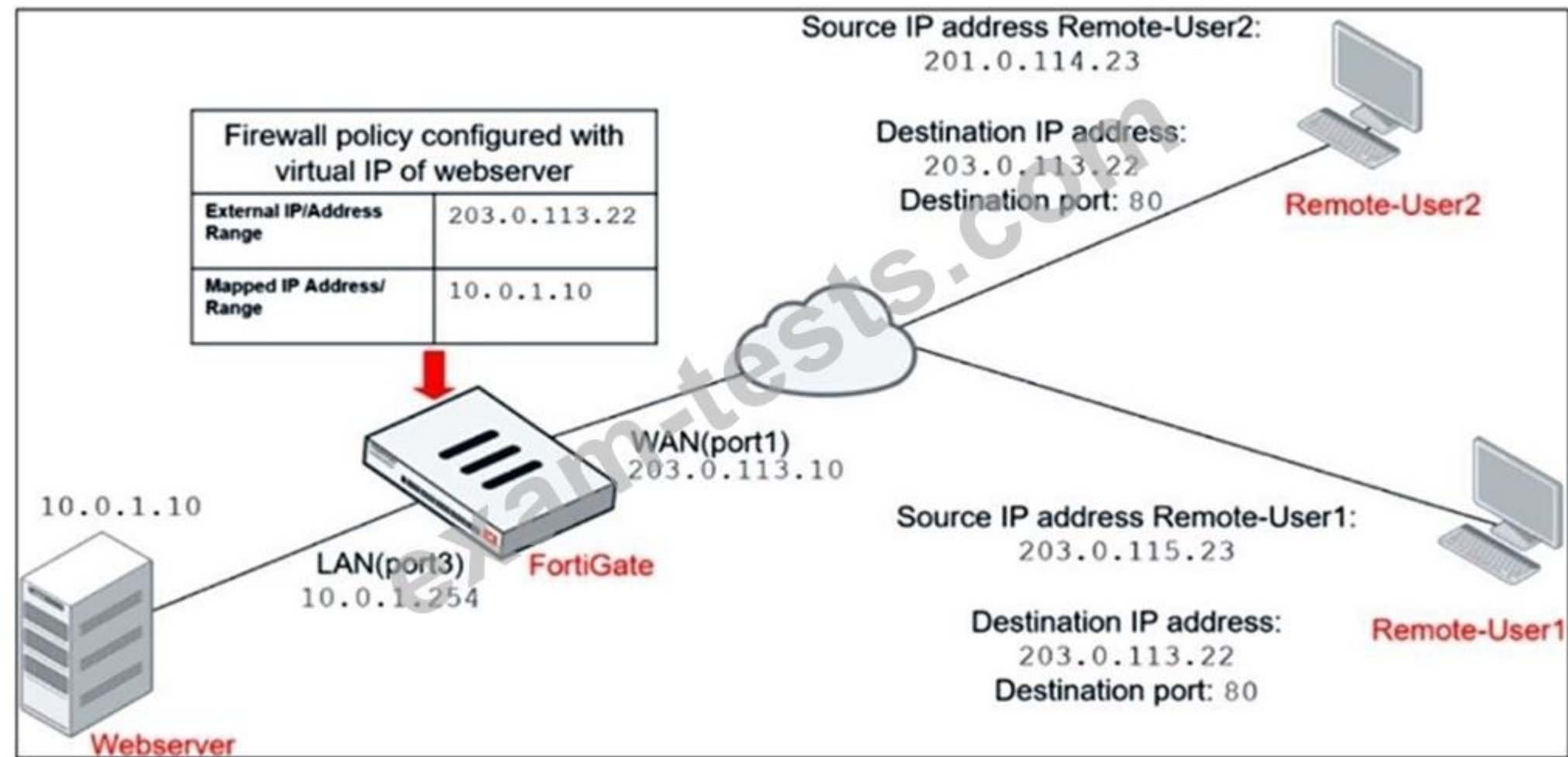
Network Protocol Enforcement settings control how FortiGate inspects and enforces protocols on traffic, including peer-to-peer applications on known ports. If not properly enabled, peer-to-peer traffic may bypass blocking despite the application control profile.

NEW QUESTION: 28

Refer to the exhibits.

Network diagram

FORTINET®



Firewall address object

Edit Address

Name

Deny_IP

Color

 Change

Type

Subnet

IP/Netmask

201.0.114.23/32

Interface

 WAN (port1)

Static route configuration

☐

Comments

Deny web server access. 23/255

Firewall policies

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

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.

The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.

Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)

- A. Set the Destination address as Webserver 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. Enable match-vip in the Deny policy.

Answer: (SHOW ANSWER)

In this scenario, the FortiGate uses a Virtual IP (VIP) to map the external IP 203.0.113.22 to the internal web server 10.0.1.10. When using VIPs, firewall policies must be configured carefully to match the translated destination address.

The external users (Remote-User1 and Remote-User2) connect to 203.0.113.22, which is the VIP for the web server.

By default, firewall policies match pre-NAT addresses (the original destination before VIP translation).

To make the deny policy recognize traffic destined for the VIP-mapped address, the match-vip option must be enabled.

The destination in the Deny policy should explicitly be the Webserver (the VIP object), so FortiGate correctly identifies the target.

NEW QUESTION: 29

You have configured the below commands on a FortiGate.

```
config system settings
set strict-src-check enable
end

Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

- A. FortiGate will enable strict RPF on all its interfaces and port1 will be enabled for asymmetric routing.
- B. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
- C. Port1 will be enabled with flexible RPF, and all other interfaces will be enabled for strict RPF
- D. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.

Answer: B ([LEAVE A REPLY](#))

The global setting enables strict source checking (RPF) on all interfaces by default. The per- interface setting disables the source check on port1, exempting it from strict RPF enforcement.

NEW QUESTION: 30

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.

Which DPD mode on FortiGate meets this requirement?

- A. On Demand
- B. Disabled
- C. On Idle
- D. Enabled

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 31

Refer to the exhibits. An administrator configured the Web Filter Profile to block access to all social networking sites except Facebook. However, when users try to access Facebook.com, they are redirected to a FortiGuard web filtering block page.

Based on the exhibits, which configuration change must the administrator make to allow Facebook while blocking all other social networking sites?

Web filter configuration

Edit Web Filter Profile

Feature set **Flow-based** Proxy-based

☒ FortiGuard Category Based Filter

☒ Allow ☒ Monitor ☐ Block ☐ Warning ☐ Authenticate

Name	Action
Web-based Applications	☒ Allow
Entertainment	☒ Allow
Arts and Culture	☒ Allow
Education	☒ Allow
Health and Wellness	☒ Allow
Job Search	☒ Allow
Medicine	☒ Allow
News and Media	☒ Allow
Social Networking	☐ Block

53% 95

☐ Allow users to override blocked categories

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☐

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

[+ Create New](#) [Edit](#) [Delete](#)

URL	Type	Action	Status
www.facebook.com	Wildcard	☒ Monitor	☒ Enable



- A. Change the type as Simple in the Static URL Filter section.
- B. Set the Social Networking action as warning in the FortiGuard Category Based Filter.
- C. Change the Feature set of Web Filter Profile as Proxy-based.
- D. Set the Action as Exempt for www.facebook.com in the Static URL Filter.

Answer: D (LEAVE A REPLY)

The FortiGuard category filter is blocking Social Networking, which includes Facebook. Although a static URL filter entry for www.facebook.com exists, its action is set to Monitor, so it does not override the category block. To allow Facebook while blocking other social networking sites, the action for www.facebook.com in the Static URL Filter must be set to Exempt. This explicitly bypasses category filtering for that URL.

Valid FCP_FGT_AD-7.6 Dumps shared by BraindumpsPass.com for Helping Passing FCP_FGT_AD-7.6 Exam! BraindumpsPass.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the BraindumpsPass.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com FCP_FGT_AD-7.6 dumps with Test Engine here: https://www.braindumpsPASS.com/Fortinet/FCP_FGT_AD-7.6-practice-exam-dumps.html (132 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 32

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

- A. The Underlay zone is the zone by default.
- B. The Underlay zone contains no member.
- C. port2 and port3 are not assigned to a zone.
- D. The virtual-wan-link and overlay zones can be deleted.

Answer: B (LEAVE A REPLY)

Underlay is not a default zone. It is user defined and not active.

NEW QUESTION: 33

Refer to the exhibits.

System Performance output



```
# 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.

Based on the system performance output, what are the two possible outcomes? (Choose two.)

- A. FortiGate has entered conserve mode.
- B. Administrators can access FortiGate only through the console port.
- C. Administrators can change the configuration.
- D. FortiGate drops new sessions.

Answer: (SHOW ANSWER)

Since memory usage is at 90%, exceeding the red threshold (88%), FortiGate enters a state where configuration changes are still allowed.

In this state, FortiGate drops new sessions to preserve resources and maintain stability.

NEW QUESTION: 34

You have created a web filter profile named restrict_media-profile with a daily category usage quota. When you are adding the profile to the firewall policy, the restrict_media-profile is not listed in the available web profile drop down.

What could be the reason?

- A. The firewall policy is in no-inspection mode instead of deep-inspection.
- B. The inspection mode in the firewall policy is not matching with web filter profile feature set.
- C. The web filter profile is already referenced in another firewall policy.
- D. The naming convention used in the web filter profile is restricting it in the firewall policy.

Answer: B ([LEAVE A REPLY](#))

Web filter profiles with category usage quotas require the firewall policy to be in proxy-based (deep) inspection mode; if the inspection mode does not match this requirement, the profile will not appear in the drop-down list.

NEW QUESTION: 35

Refer to the exhibit showing a debug flow output.

```
Debug Flow output
vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0
from port4, type=8, code=0, id=3, seq=5.
allocate a new session-00000721
in-[port4], out=[]
len=0
result_skb_flags-02000000, vid-0, ret-no-match, act-accept, flag-00000000
find a route: flag=00000000 gw-0.0.0.0 via port2
in[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, uri_cat_id: 0
gnum-100004, use addr/ntf hash, len=3
checked gnum-100004 policy-2, ret-matched, act-accept
ret-matched
gnum-4e20, check-fffffa002c9c7
checked gnum-4e20 policy-6, ret-no-match, act-accept
gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000
policy-2 is matched, act-drop
after iprobe_captive_check(): is_captive-0, ret-matched, act-drop, idx-2
Denied by forward policy check (policy 2)
```

Which two conclusions can you make from the debug flow output? (Choose two.)

- A. The RPF check fails.
- B. The debug flow is for UDP traffic.
- C. The matching firewall policy denies the traffic.
- D. The default gateway is configured on port2.

Answer: C,D ([LEAVE A REPLY](#))

NEW QUESTION: 36

A network administrator enabled antivirus and selected an SSL inspection profile on a firewall policy. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and does not block the file, allowing it to be downloaded.

The administrator confirms that the traffic matches the configured firewall policy. What are two reasons for the failed virus detection by FortiGate? (Choose two.)

- A. The website is exempted from SSL inspection.
- B. The selected SSL inspection profile has certificate inspection enabled.
- C. The EICAR test file exceeds the protocol options oversize limit.
- D. The browser does not trust the FortiGate self-signed CA certificate.

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 37

An administrator configured a FortiGate device to act as a collector for agentless polling mode.

What must the administrator add to the FortiGate device to retrieve AD user group information?

- A. TACACS server
- B. LDAP server
- C. RADIUS server
- D. Keycloak server

Answer: B ([LEAVE A REPLY](#))

In agentless polling mode, FortiGate directly queries Active Directory to obtain user and group information. To do this, the administrator must configure an LDAP server on the FortiGate, which allows it to retrieve user group membership details from AD.

NEW QUESTION: 38

A network administrator is reviewing firewall policies in both Interface Pair View and By Sequence View. The policies appear in a different order in each view.

Why is the policy order different in these two views?

- A. Policies in Interface Pair View are prioritized by security levels, while By Sequence View strictly follows the administrator's manual ordering.
- B. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
- C. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
- D. Interface Pair View sorts policies based on matching interfaces, while By Sequence View shows the actual processing order of rules.

Answer: D ([LEAVE A REPLY](#))

Interface Pair View organizes policies grouped by source and destination interfaces, whereas By Sequence View displays policies in the exact order they are processed by the firewall.

NEW QUESTION: 39

An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.

What is true about the DNS connection to a FortiGuard server?

- A. It uses DNS over TLS.
- B. It uses DNS over HTTPS.
- C. It uses UDP 8888.
- D. It uses UDP 53.

Answer: ([SHOW ANSWER](#)**)**

When FortiGuard servers are configured as DNS servers on FortiGate with default settings, the DNS queries are sent using the standard DNS protocol over UDP port 53.

NEW QUESTION: 40

Which two settings are required for SSL VPN to function between two FortiGate devices?

(Choose two.)

- A. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.
- B. The client FortiGate requires a manually added route to remote subnets.
- C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
- D. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.

Answer: ([SHOW ANSWER](#))

The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

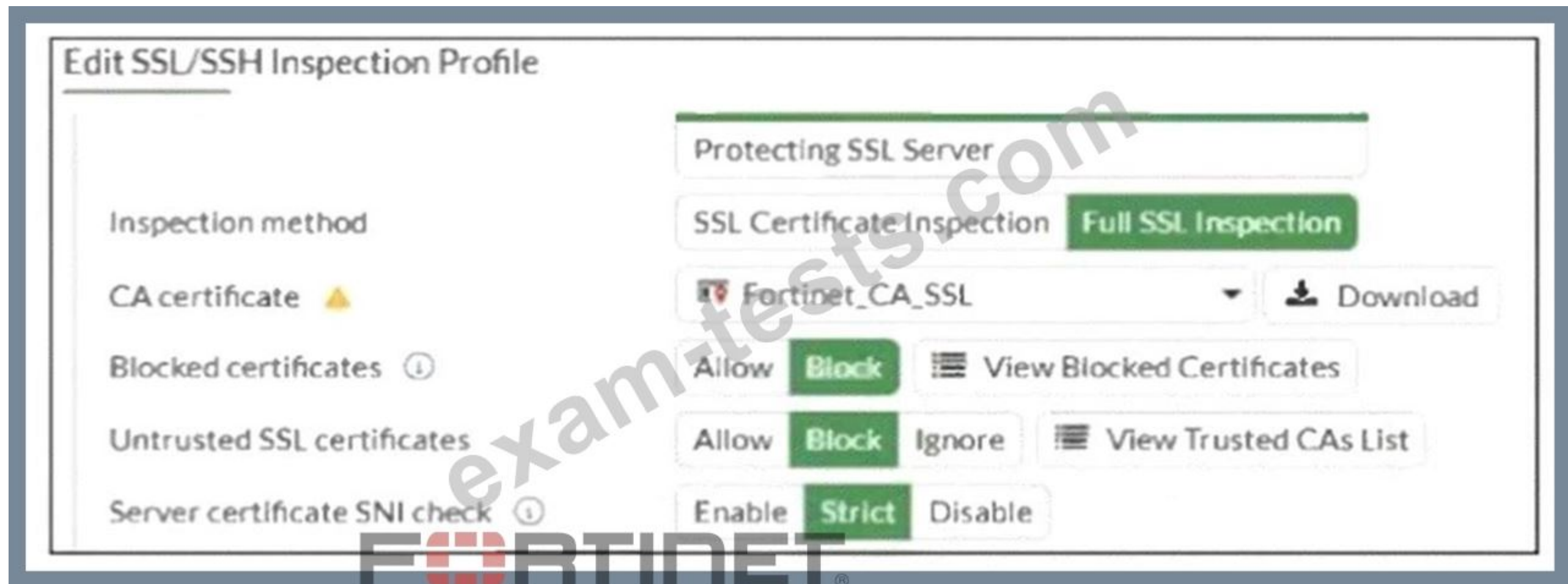
When configuring an SSL VPN tunnel between two FortiGates, the server FortiGate must verify the authenticity of the connecting client's certificate. This is done using a CA certificate installed on the server to ensure the client certificate is trusted.

The client FortiGate requires a client certificate signed by the CA on the server FortiGate.

The client FortiGate uses this client certificate to authenticate itself to the server during SSL VPN negotiation. The certificate must be signed by the same CA trusted by the server to establish a secure, validated SSL VPN connection.

NEW QUESTION: 41

Refer to the exhibit.



What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

- A. FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.
- B. FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
- C. FortiGate will close the connection if the SNI does not match the CN or SAN fields.

D. FortiGate will close the connection if the SNI does not match the CN and SAN fields

Answer: D ([LEAVE A REPLY](#))

With the Server certificate SNI check set to Strict, FortiGate enforces that the SNI must match either the Common Name (CN) or Subject Alternative Name (SAN) in the server certificate; otherwise, it closes the connection.

NEW QUESTION: 42

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A.** They rely on session loss and jitter.
- B.** They can be measured actively or passively.
- C.** They are applied in a SD-WAN rule lowest cost strategy.
- D.** They monitor the state of the FortiGate device.
- E.** All the SLA targets can be configured.

Answer: A,B,E ([LEAVE A REPLY](#))

SD-WAN SLAs monitor metrics like packet loss and jitter to evaluate link performance. SLA measurements can be performed using active probing or passive monitoring. Administrators can configure all SLA target parameters to define performance criteria.

NEW QUESTION: 43

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

- A.** The collector agent uses a Windows API to query DCs for user logins.
- B.** NetAPI polling can increase bandwidth usage in large networks.
- C.** The NetSessionEnum function is used to track user logouts.
- D.** The collector agent must search Windows application event logs.

Answer: ([SHOW ANSWER](#)**)**

NetAPI polling mode involves frequent queries to domain controllers, which can cause increased bandwidth usage, especially in large networks with many login events.

NEW QUESTION: 44

Refer to the exhibits.

Network diagram

NAT IP pool configuration

Name	External IP Range	Type	ARP Reply
SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) ③							
TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT
PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1	NAT
IGMP traffic (4)	all	all	always	IGMP	ACCEPT	SNAT-Remote	NAT

The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.

The WAN (port2) interface has the IP address 100.65.0.101/24.

The LAN (port4) interface has the IP address 10.0.11.254/24.

Which IP address will be used to source NAT (SNAT) the traffic, if the user on HQ-PC-1 (10.0.11.50) pings the IP address of BR-FGT (100.65.1.111)

- A. 100.65.0.101
- B. 100.65.0.49
- C. 100.65.0.99
- D. 100.65.0.149

Answer: C (LEAVE A REPLY)

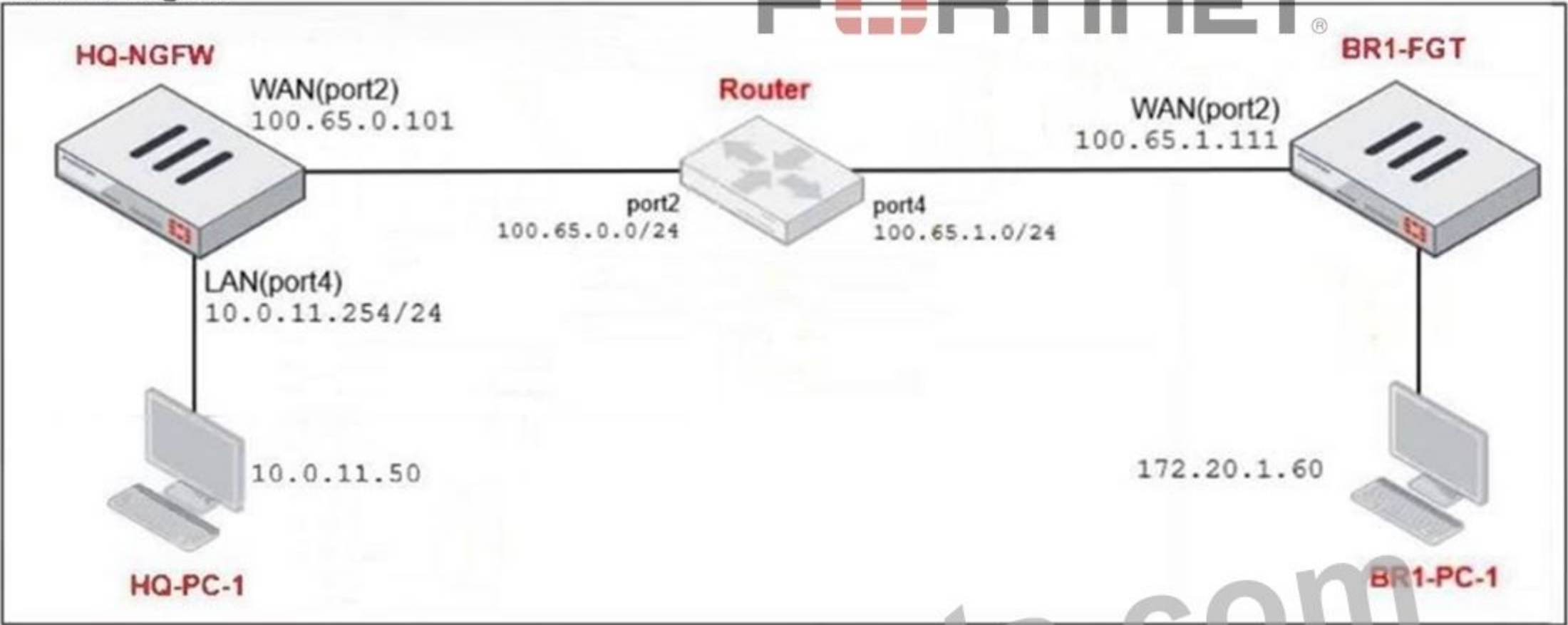
The ping traffic policy uses the IP pool named SNAT-Remote1, which has the external IP range 100.65.0.99. Therefore, traffic matching this policy (ping from HQ-PC-1 to BR1-FGT) will use

100.65.0.99 for source NAT.

NEW QUESTION: 45

Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, as well as the IP pool configuration and firewall policy objects.

Network diagram



NAT IP pool configuration

	Name	External IP Range	Type	ARP Reply
☐	SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	Enabled
☐	SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	Enabled
☐	SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
☐ TCP traffic (2)	4 all	4 BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool	NAT

☐	PING traffic (3)	4 all	4 all	always	PING	✓ ACCEPT	SNAT-Remote1	✓ NAT
☐	IGMP traffic (4)	4 all	4 all	always	IGMP	✓ ACCEPT	SNAT-Remote	✓ NAT

The WAN (port2) interface has the IP address 100.65.0.101/24. The LAN (port4) interface has the IP address 10.0.11.254/24. Which IP address will be used to source NAT (SNAT) the traffic, if the user on HQ-PC-1 (10.0.11.50) pings the IP address of BR-FGT (100.65.1.111)

- A. 100.65.0.101
- B. 100.65.0.49
- C. 100.65.0.99
- D. 100.65.0.149

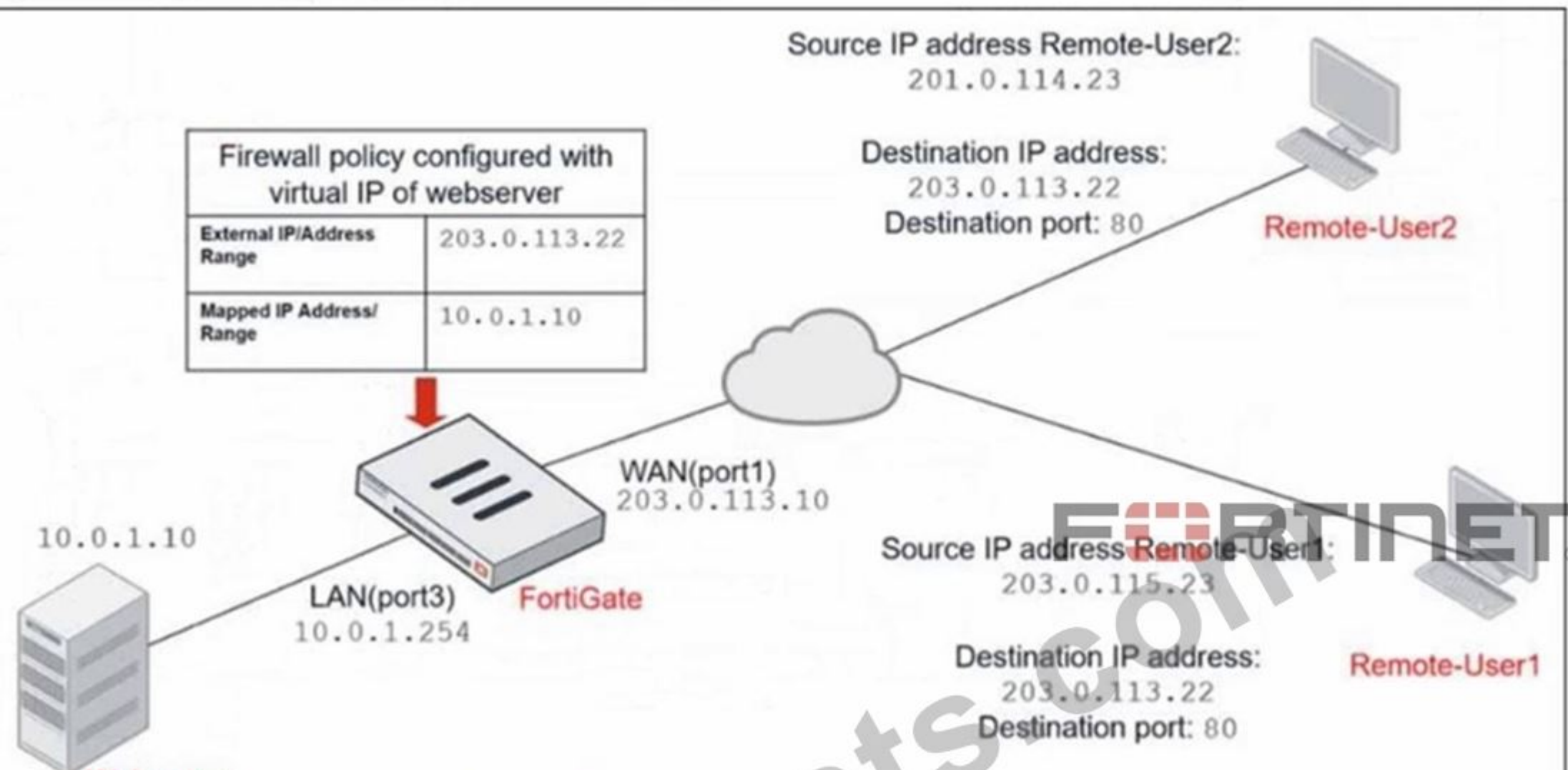
Answer: C (LEAVE A REPLY)

The ping traffic policy uses the IP pool named SNAT-Remote1, which has the external IP range 100.65.0.99. Therefore, traffic matching this policy (ping from HQ-PC-1 to BR1-FGT) will use 100.65.0.99 for source NAT.

NEW QUESTION: 46

Refer to the exhibits.

Network diagram



Firewall address object

Edit Address

Name

Deny_IP

Color

Change

Type

Subnet

IP/Netmask

201.0.114.23/32

Interface

WAN (port1)

Static route configuration

Comments

Deny web server access. 23/255

Firewall policies

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

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall configuration.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.

The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.

Which additional configuration can the administrator add to a deny firewall policy, beyond the default behavior, to block Remote-User2 from accessing the Webserver?

- A. Disable match-vip in the Allow_access policy
- B. Configure a One-to-One IP Pool object in a new policy.
- C. Set the Destination address as Webserver in the Deny policy.
- D. Set the Destination address as Deny_IP in the Allow_access policy.

Answer: C (LEAVE A REPLY)

To block Remote-User2's access to the Webserver, the deny policy must explicitly specify the Webserver as the destination address; otherwise, it denies traffic to all destinations, which is not the desired behavior.

Valid FCP_FGT_AD-7.6 Dumps shared by BraindumpsPass.com for Helping Passing FCP_FGT_AD-7.6 Exam! BraindumpsPass.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the BraindumpsPass.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com FCP_FGT_AD-7.6 dumps with Test Engine here: https://www.braindumpspass.com/Fortinet/FCP_FGT_AD-7.6-practice-exam-dumps.html (132 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode.

Which step is NOT part of the expected process?

- A.** The DC agent sends login event data directly to FortiGate.
- B.** The user logs into the windows domain.
- C.** The collector agent forwards login event data to FortiGate.
- D.** FortiGate determines user identity based on the IP address in the FSSO list.

Answer: C ([LEAVE A REPLY](#))

In DC Agent Mode, the DC agent sends login event data directly to FortiGate without involving a collector agent.

NEW QUESTION: 48

Refer to the exhibits.

System Performance output

```
# 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
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-extreme 89
    set memory-use-threshold-green 82
    set memory-use-threshold-red 88
end
```

FORTINET®

The exhibits show the system performance output and default configuration of high memory usage thresholds on a FortiGate device.

Based on the system performance output, what are the two possible outcomes? (Choose two.)

- A. FortiGate has entered conserve mode.
- B. Administrators can access FortiGate only through the console port.
- C. Administrators can change the configuration.
- D. FortiGate drops new sessions.

Answer: C,D (LEAVE A REPLY)

Since memory usage is at 90%, exceeding the red threshold (88%), FortiGate enters a state where configuration changes are still allowed.

In this state, FortiGate drops new sessions to preserve resources and maintain stability.

NEW QUESTION: 49

Refer to the exhibits. The exhibits show the application sensor configuration and the Excessive- Bandwidth and Apple filter details.

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

Application sensor configuration

Edit Application Sensor

Categories

▼ All Categories

- ☒ Business (179, ☁ 6)
- ☒ Collaboration (293, ☁ 6)
- ☐ Game (124)
- ☐ Mobile (3)
- ☐ P2P (85)
- ☐ Remote.Access (91)
- ☒ Storage.Backup (296, ☁ 16)
- ☐ Video/Audio (206, ☁ 13)
- ☐ Web.Client (18)
- ☒ Cloud.IT (31)
- ☒ Email (87, ☁ 12)
- ☒ General.Interest (241, ☁ 9)
- ☒ Network.Service (332)
- ☐ Proxy (106)
- ☐ Social.Media (150, ☁ 31)
- ☒ Update (48)
- ☐ VoIP (30)
- ☐ Unknown Applications

☐ Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	Excessive-Bandwidth	Filter	Block
2	Apple	Filter	Monitor

Application override configuration

The screenshot shows the 'Edit Override' configuration for FaceTime. The 'Type' is set to 'Application' and the 'Filter' is 'BHVR Excessive-Bandwidth'. The 'Action' is 'Block'. The 'Name' field contains 'FaceTime'. Below the configuration, a table lists the override details:

Name	Category	Technology
FaceTime	VoIP	Client-Server

The table also shows 'Application Signature 1/1262'.

Filter override configuration

The screenshot shows the 'Edit Override' configuration for FaceTime. The 'Type' is set to 'Application' and the 'Filter' is 'VEND Apple'. The 'Action' is 'Monitor'. The 'Name' field contains 'FaceTime'. Below the configuration, a table lists the override details:

Name	Category	Technology
FaceTime	VoIP	Client-Server

The table also shows 'Application Signature 1/33'.

- A. Apple Face Time will be allowed, based on the Video/Audio category configuration.
- B. Apple Face Time will be blocked, based on the Excessive-Bandwidth filter configuration.
- C. Apple Face Time will be allowed, based on the Apple filter configuration.
- D. Apple Face Time will be allowed only if the Apple filter in Application and Filter Overrides is set to Allow.

Answer: C (LEAVE A REPLY)

Apple FaceTime normally falls under Video/Audio and could be blocked by the Excessive- Bandwidth filter. However, in this configuration, an override is applied under the Apple vendor filter with Monitor action. Overrides take precedence over general filter actions. Therefore, FaceTime will not be blocked; instead, it will be monitored, and since only a few calls are made (not excessive bandwidth usage), it will be allowed based on the Apple filter configuration.

NEW QUESTION: 50

FortiGate is operating in NAT mode and has two physical interfaces connected to the LAN and DMZ networks respectively.

Which two statements about the requirements of connected physical interfaces on FortiGate are true? (Choose two.)

- A. Both interfaces must have IP addresses assigned.
- B. Both interfaces must have DHCP enabled and interfaces set to LAN and DMZ roles assigned.
- C. Both interfaces must have the interface role assigned.
- D. Both interfaces must have directly connected routes on the routing table.

Answer: ([SHOW ANSWER](#))

Interfaces must have directly connected routes in the routing table to forward traffic correctly.

Interfaces must have IP addresses assigned to communicate within their respective networks.

NEW QUESTION: 51

Which three statements about SD-WAN performance SLAs are true? (Choose three.)

- A. They rely on session loss and jitter.
- B. They can be measured actively or passively.
- C. They are applied in a SD-WAN rule lowest cost strategy.
- D. They monitor the state of the FortiGate device.
- E. All the SLA targets can be configured.

Answer: A,B,E ([LEAVE A REPLY](#))

SD-WAN SLAs monitor metrics like packet loss and jitter to evaluate link performance.

SLA measurements can be performed using active probing or passive monitoring.

Administrators can configure all SLA target parameters to define performance criteria.

NEW QUESTION: 52

You have configured the below commands on a FortiGate.

A screenshot of a FortiGate CLI session showing two configuration blocks. The first block is 'config system settings' followed by 'set strict-src-check enable' and 'end'. The second block is 'Config system interface' followed by 'edit port1', 'set src-check disable', 'next', and 'end'. A watermark 'examtests.com' is visible across the text.

```
config system settings
set strict-src-check enable
end

Config system interface
edit port1
set src-check disable
next
end
```

What would be the impact of this configuration on FortiGate?

- A. FortiGate will enable strict RPF on all its interfaces and port1 will be enabled for asymmetric routing.
- B. FortiGate will enable strict RPF on all its interfaces and port1 will be exempted from RPF checks.
- C. Port1 will be enabled with flexible RPF, and all other interfaces will be enabled for strict RPF
- D. The global configuration will take precedence and FortiGate will enable strict RPF on all interfaces.

Answer: B ([LEAVE A REPLY](#))

The global setting enables strict source checking (RPF) on all interfaces by default. The per-interface setting disables the source check on port1, exempting it from strict RPF enforcement.

NEW QUESTION: 53

A new administrator is configuring FSSO authentication on FortiGate using DC Agent Mode.

Which step is NOT part of the expected process?

- A. The DC agent sends login event data directly to FortiGate.

- B. The user logs into the windows domain.
- C. The collector agent forwards login event data to FortiGate.
- D. FortiGate determines user identity based on the IP address in the FSSO list.

Answer: A (LEAVE A REPLY)

In DC Agent Mode, the DC agent sends login event data directly to FortiGate without involving a collector agent.

NEW QUESTION: 54

Refer to the exhibit.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port3 → port1 1									
1	Full_Access	Remote-users LOCAL_SUB...	all	always	HTTP HTTPS ALL_ICMP	ACCEPT	NAT	Standard	Category_Monitor certificate-inspection

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt.

What is the most likely reason for this situation?

- A. The Service DNS is required in the firewall policy.
- B. The user is using an incorrect user name.
- C. No matching user account exists for this user.
- D. The Remote-users group is not added to the Destination.

Answer: A (LEAVE A REPLY)

In FortiGate firewall authentication, users are prompted for login credentials only when their initial request matches a policy requiring authentication.

In this configuration, the firewall policy permits HTTP, HTTPS, and ICMP traffic, but DNS service is missing.

Since browsers first need DNS resolution before sending HTTP/HTTPS requests, the user cannot reach the FortiGate for authentication.

Adding DNS to the Service field (Option A) enables the user to resolve hostnames and trigger the firewall authentication prompt.

NEW QUESTION: 55

Refer to the exhibits.

SSL-VPN settings

SSL-VPN Settings

Connection Settings ⓘ

Enable SSL-VPN ☒

Listen on Interface(s)

port1 +

Listen on Port

11443

Web mode access will be listening at https://10.200.1.1:11443

Server Certificate

Fortinet_Factory

Redirect HTTP to SSL-VPN ☐

Restrict Access

Allow access from any host Limit access to specific hosts

Idle Logout ☒

Inactive For

300

Seconds

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 ☐

Web Mode Settings

Language

Browser Preference System

Authentication/Portal Mapping

+ Create New Edit Delete Send SSL-VPN Configuration	
Users/Groups	Portal
SSL-VPN-Users	tunnel-access
All Other Users/Groups	full-access
2	

FORTINET®



The SSL VPN connection fails when a user attempts to connect to it.

What should the user do to successfully connect to the SSL VPN?

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

Answer: ([SHOW ANSWER](#))

In the FortiGate SSL-VPN settings, the VPN is configured to listen on port 11443, as shown in the

"Listen on Port" field. However, the VPN client is attempting to connect to https://10.200.1.1:443/, which uses the default HTTPS port (443) instead of the configured port.

To successfully connect, the user must change the SSL VPN port on the client to 11443 so that it matches the listening port defined on the FortiGate device.

NEW QUESTION: 56



Refer to the exhibits.

An administrator configured the Web Filter Profile to block access to all social networking sites except Facebook. However, when users try to access Facebook.com, they are redirected to a FortiGuard web filtering block page.

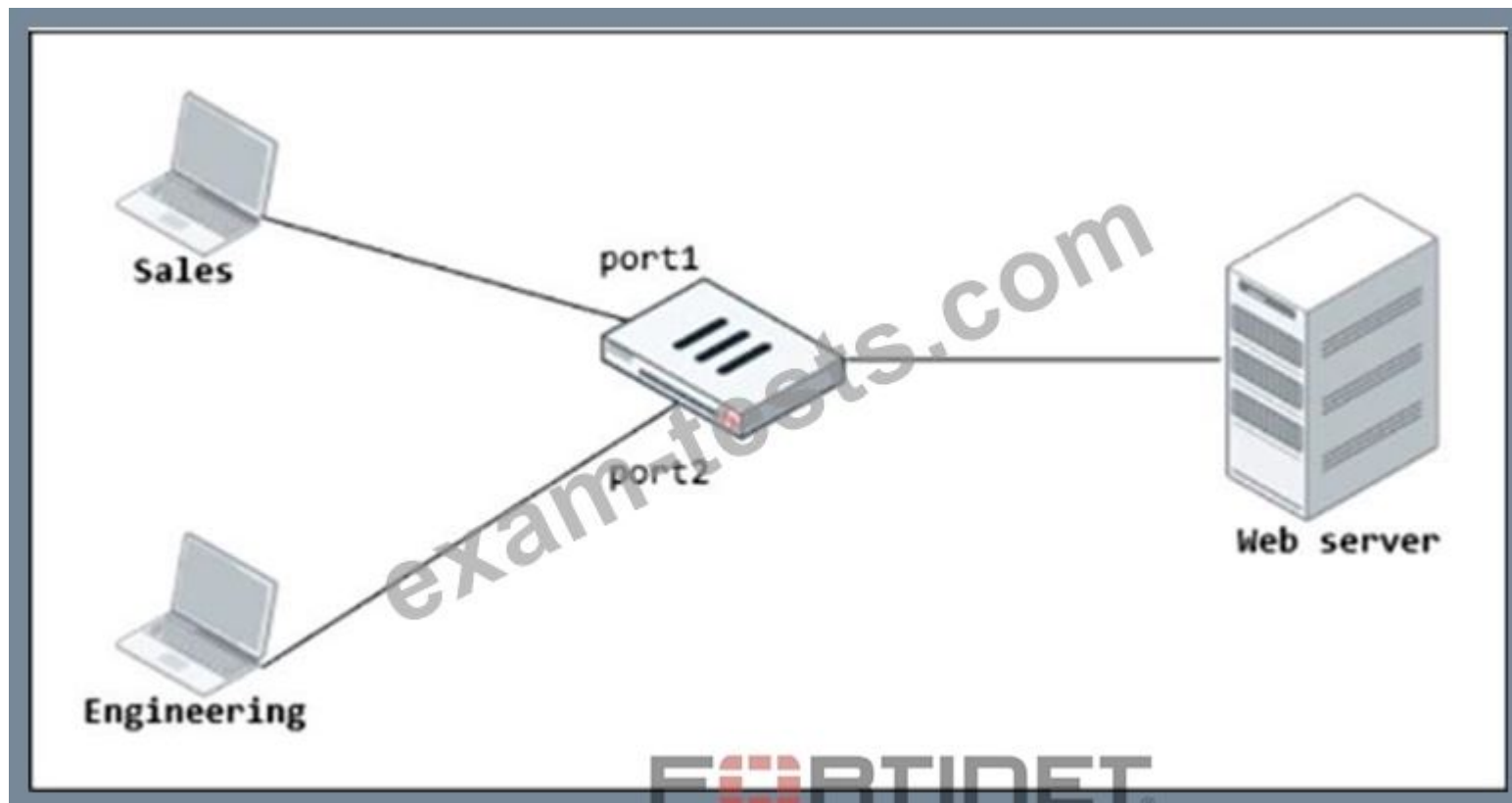
Based on the exhibits, which configuration change must the administrator make to allow Facebook while blocking all other social networking sites?

- A. Change the type as Simple in the Static URL Filter section.
- B. Set the Action as Exempt for www.facebook.com in the Static URL Filter.
- C. Change the Feature set of Web Filter Profile as Proxy-based.
- D. Set the Social Networking action as warning in the FortiGuard Category Based Filter.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 57

Refer to the exhibit.



FortiGate has two separate firewall policies for Sales and Engineering to access the same web server with the same security profiles.

Which action must the administrator perform to consolidate the two policies into one?

- A. Create an Interface Group that includes port1 and port2 to create a single firewall policy.
- B. Enable Multiple Interface Policies to select port1 and port2 in the same firewall policy.
- C. Replace port1 and port2 with the any interface in a single firewall policy.
- D. Select port1 and port2 subnets in a single firewall policy.

Answer: A (LEAVE A REPLY)

To consolidate two firewall policies that use different incoming interfaces (port1 and port2) but have the same destination, services, and security profiles, the administrator should create an Interface Group that includes both port1 and port2.

This allows a single firewall policy to apply to traffic from both interfaces, simplifying management while maintaining consistent security enforcement.

NEW QUESTION: 58

Refer to the exhibit.

+ Create New Edit Delete			
Priority	Details	Type	Action
1	ABC.Com	Application	Allow
2	Excessive-Bandwidth	Filter	Block

An administrator has configured an Application Overrides for the ABC.Com application signature and set the Action to Allow. This application control profile is then applied to a firewall policy that is scanning all outbound traffic. Logging is enabled in the firewall policy. To test the configuration, the administrator accessed the ABC.Com web site several times.

Why are there no logs generated under security logs for ABC.Com?

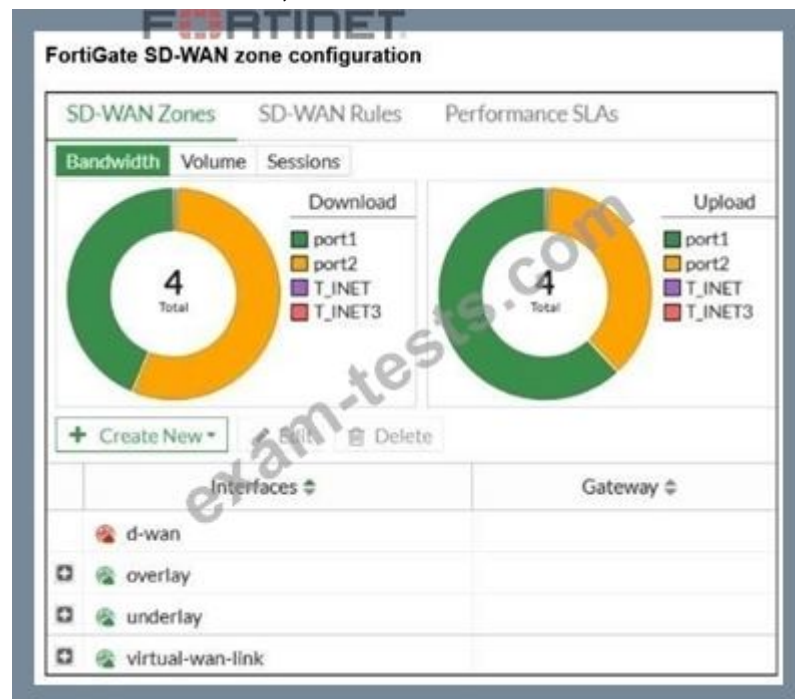
- A. The ABC.Com Type is set as Application instead of Filter.
- B. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
- C. The ABC.Com Action is set to Allow.
- D. The ABC.Com is hitting the category Excessive-Bandwidth.

Answer: C (LEAVE A REPLY)

When the action is set to Allow in an application override, traffic matching this override is allowed without generating security logs because it bypasses deeper inspection and blocking.

NEW QUESTION: 59

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

- A. The underlay zone contains port1 and port2.
- B. The d-wan zone contains no member.
- C. The d-wan zone cannot be deleted.
- D. The virtual-wan-link zone contains no member.

Answer: B (LEAVE A REPLY)

The "d-wan" zone in FortiGate SD-WAN configuration is the default SD-WAN zone created when SD-WAN is enabled. This zone contains all the interfaces assigned to SD-WAN and is essential for the functionality of the SD-WAN feature. The "d-wan" zone cannot be deleted because it is required for SD-WAN operations. Option A is incorrect because the underlay zone does not contain port1.

NEW QUESTION: 60

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.



Based on the exhibit, which statement is true?

- A. The Underlay zone is the zone by default.
- B. The Underlay zone contains no member.
- C. port2 and port3 are not assigned to a zone.
- D. The virtual-wan-link and overlay zones can be deleted.

Answer: A (LEAVE A REPLY)

The Underlay zone is the default SD-WAN zone, typically representing the physical interfaces in the SD-WAN configuration before overlay or virtual links are added.

NEW QUESTION: 61

You are encountering connectivity problems caused by intermediate devices blocking IPsec traffic.

In which two ways can you effectively resolve the problem? (Choose two.)

- A. You can use SSL VPN tunnel mode to prevent problems with blocked ESP and UDP ports (500 or 4500).
- B. You can configure a hub-and-spoke topology with SSL VPN tunnels to bypass blocked UDP ports.
- C. You should use the protocol IKEv2.
- D. You can turn on fragmentation to fix large certificate negotiation problems.

Answer: A,D (LEAVE A REPLY)

Valid FCP_FGT_AD-7.6 Dumps shared by BraindumpsPass.com for Helping Passing FCP_FGT_AD-7.6 Exam! BraindumpsPass.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the BraindumpsPass.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com FCP_FGT_AD-7.6 dumps with Test Engine here: https://www.braindumpsPass.com/Fortinet/FCP_FGT_AD-7.6-practice-exam-dumps.html (132 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 62

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

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 63

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 must the administrator make on FortiGate to meet the requirements? (Choose two.)

- A. In the phase1-interface, enable npu-offload to detect a dead tunnel.
- B. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- C. Enable Dead Peer Detection.
- D. Use the VPN wizard to create an IPsec template for a redundant IPsec VPN tunnel.

Answer: B,C (LEAVE A REPLY)

Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel → This ensures that the primary tunnel is always preferred, and the secondary is only used when the primary route is unavailable.
Enable Dead Peer Detection → DPD allows FortiGate to quickly detect when the primary tunnel is down, enabling faster failover to the backup tunnel.

NEW QUESTION: 64



Refer to the exhibits.
An administrator configured the Web Filter Profile to block access to all social networking sites except Facebook. However, when users try to access Facebook.com, they are redirected to a FortiGuard web filtering block page.
Based on the exhibits, which configuration change must the administrator make to allow Facebook while blocking all other social networking sites?

- A. Set the Social Networking action as warning in the FortiGuard Category Based Filter.
- B. Change the Feature set of Web Filter Profile as Proxy-based.
- C. Change the type as Simple in the Static URL Filter section.
- D. Set the Action as Exempt for www.facebook.com in the Static URL Filter.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 65

An administrator wants to configure dead peer detection (DPD) on IPsec VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when there is no inbound traffic.

Which DPD mode on FortiGate meets this requirement?

- A. Enabled
- B. On Idle
- C. Disabled
- D. On Demand

Answer: A (LEAVE A REPLY)

The "On Idle" DPD mode configures FortiGate to send DPD probes only when no inbound traffic is detected, meeting the requirement to send probes only when the tunnel is idle.

NEW QUESTION: 66

Refer to the exhibits. A web filter profile configuration and firewall policy configuration are shown. You are trying to access www.facebook.com, but you are redirected to a FortiGuard web filtering block page. Based on the exhibits, what is the possible cause of the issue?

Web filter profile configuration

Edit Web Filter Profile

Feature set

Flow-based

Proxy-based

☒ FortiGuard Category Based Filter

✔ Allow

👁 Monitor

🚫 Block

⚠ Warning

👤 Authenticate

Name	Action
Job Search	✔ Allow
Medicine	✔ Allow
News and Media	✔ Allow
Social Networking	✔ Allow
Political Organizations	✔ Allow

Reference	☒ Allow
Global Religion	☒ Allow
Shopping	☒ Allow
Society and Lifestyles	☒ Allow

58% 95

☐ Allow users to override blocked categories

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex ☐

Static URL Filter

Block invalid URLs ☐

URL Filter ☒

+ Create New
Edit
Delete
Search

URL	Type	Action	Status
www.facebook.com	Simple	☒ Monitor	☒ Enable

Firewall policy configuration

Edit Policy

Firewall / Network Options

Inspection Mode ☒ Flow-based ☐ Proxy-based

NAT ☒

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Preserve Source Port ☐

Protocol Options ☒ PROX default

Security Profiles

AntiVirus ☐

Web Filter ☒ WEB default

IPS ☐

File filter ☐

SSL inspection ☒ SSL certificate-inspection



- A. The web filter profile feature set is configured incorrectly.
- B. The web rating override configuration is incorrect.
- C. The firewall policy inspection mode is incorrect.
- D. For www.facebook.com, the URL filter action is incorrect.

Answer: (SHOW ANSWER)

The web filter profile shows a URL filter override for www.facebook.com with action Monitor, which should allow access. However, the block page shows FortiGuard categorizing www.facebook.com as Malicious Websites and blocking it. This indicates that the web rating override configuration is incorrect (the override is not applied properly), so FortiGuard's default category action takes precedence and blocks the site.

NEW QUESTION: 67

Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

- A. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
- B. Pre-shared key and certificate signature as authentication methods
- C. No certificate is required on the remote peer when you set the certificate signature as the authentication method
- D. Extended authentication (XAuth) to request the remote peer to provide a username and password

Answer: B,D (LEAVE A REPLY)

Pre-shared key and certificate signature as authentication methods

FortiGate supports both pre-shared keys and digital certificates for IKEv1 authentication, providing flexibility in securing IPsec VPN tunnels.

Extended authentication (XAuth) to request the remote peer to provide a username and password FortiGate supports XAuth in IKEv1 to add an extra layer of user-level authentication, where the remote peer must provide a username and password in addition to the IKE credentials.

NEW QUESTION: 68
Refer to the exhibit.



Phase 2 selectors

Create new

Edit

Delete

Search

Name	Local Address	Remote Address	Comments
ToBR1	10.0.11.0/255.255.255.0	172.20.1.0/255.255.255.0	

Edit Phase 2 Selector

Name

ToBR1

Comments

Comments

Encapsulation

Tunnel Mode

Transport Mode

IP version

IPv4

IPv6

Named address

Local address

IP Address

Subnet Address

IP Range

Phase 2 selectors

Create new

Edit

Delete

Search

Name	Local Address	Remote Address	Comments
ToHQ	172.20.1.0/255.255.255.0	10.11.0.0/255.255.255.0	

Edit Phase 2 Selector

Name

ToHQ

Comments

Comments

Encapsulation

Tunnel Mode

Transport Mode

IP version

IPv4

IPv6

Named address

Local address

IP Address

Subnet Address

IP Range

Remote address: 10.0.11.0 255.255.255.0

Remote address: 172.20.1.0 255.255.255.0

Advanced

Encryption - authentication: AES128 - SHA1

Replay detection: ☒ Enable ☐ Disable

Perfect forward secrecy (PFS): ☒ Enable ☐ Disable

Diffie-Hellman groups:

☐ 1	☐ 2	☒ 5
☐ 14	☐ 15	☐ 16
☐ 17	☐ 18	☐ 19
☐ 20	☐ 21	☐ 27
☐ 28	☐ 29	☐ 30
☐ 31	☐ 32	

Local port: ☒ All ☐ Specify

Remote port: ☒ All ☐ Specify

Protocol: ☒ All ☐ Specify

Auto-negotiate: ☒ Enable ☐ Disable

Autokey keep alive: ☒ Enable ☐ Disable

Key lifetime: ☒ Seconds ☐ Kilobytes ☐ Both

43200 second(s)

Remote address: 172.20.1.0 255.255.255.0

Remote address: 10.11.0.0 255.255.255.0

Advanced

Encryption - authentication: AES256 - SHA1

Replay detection: ☒ Enable ☐ Disable

Perfect forward secrecy (PFS): ☒ Enable ☐ Disable

Diffie-Hellman groups:

☐ 1	☐ 2
☒ 14	☐ 15
☐ 17	☐ 18
☐ 20	☐ 21
☐ 28	☐ 29
☐ 31	☐ 32

Local port: ☒ All ☐ Specify

Remote port: ☒ All ☐ Specify

Protocol: ☒ All ☐ Specify

Auto-negotiate: ☒ Enable ☐ Disable

Autokey keep alive: ☒ Enable ☐ Disable

Key lifetime: ☒ Seconds ☐ Kilobytes ☐ Both

14400

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, which two configuration changes will bring phase 2 up? (Choose two.)

- A. On BR1-FGT, set Seconds to 43200.
- B. On HQ-NGFW, enable Diffie-Hellman Group 2.
- C. On BR1-FGT, set Remote Address to 10.0.11.0/255.255.255.0

D. On HQ-NGFW. set Encryption to AES256

Answer: A,C ([LEAVE A REPLY](#))

The key lifetime (Seconds) must match on both sides; BR1-FGT is set to 14400, so setting it to 43200 matches HQ-NGFW.

The remote address on BR1-FGT should match the HQ-NGFW's local subnet (10.0.11.0/24), but it is currently set incorrectly as 172.20.1.0/24. Changing it to 10.0.11.0/255.255.255.0 will align the Phase 2 selectors.

NEW QUESTION: 69

Which two statements are true about an HA cluster? (Choose two.)

A. An HA cluster cannot have both in-band and out-of-band management interfaces at the same time.

B. Link failover triggers a failover if the administrator sets the interface down on the primary device.

C. When sniffing the heartbeat interface, the administrator must see the IP address 169.254.0.2.

D. HA incremental synchronization includes FIB entries and IPsec SAs.

Answer: B,D ([LEAVE A REPLY](#))

Setting an interface down on the primary device triggers a failover due to link failover detection.

HA incremental synchronization includes forwarding information base (FIB) entries and IPsec security associations (SAs) to maintain session continuity.

NEW QUESTION: 70

Refer to the exhibit showing a debug flow output.

Debug Flow output

vd-root:0 received a packet(proto=1, 10.0.11.50:3->100.65.0.254:2048) tun_id=0.0.0.0 from port4, type=8, code=0, id=3, seq=5.

allocate a new session-00000721

in-[port4], out-[]

len=0

result:skb_flags-02000000, vid-0, ret no-match, act-accept, flag-00000000

find a route: flag=00000000 gw-0.0.0.0 via port2

in[port4], out-[port2], skb_flags-02000000, vid-0, app_id: 0, url_cat_id: 0

gnum-100004, use addr/intf hash, len=3

checked gnum-100004 policy-2, ret-matched, act-accept

ret-matched

gnum-4e20, check-fffffa002c9c7

checked gnum-4e20 policy-6, ret-no-match, act-accept

gnum-4e20 check result: ret-no-match, act-accept, flag-00000000, flag2-00000000

policy-2 is matched, act-drop

after iprobe_captive_check(): is_captive-0, ret-matched, act-drop, idx-2

Denied by forward policy check (policy 2)

Which two conclusions can you make from the debug flow output? (Choose two.)

- A. The default gateway is configured on port2.
- B. The RPF check fails.

- C. The debug flow is for UDP traffic.
- D. The matching firewall policy denies the traffic.

Answer: A,D ([LEAVE A REPLY](#))

The default gateway is configured on port2 → The debug output shows find a route:

flag=00000000 gw=0.0.0.0 via port2, which indicates that the default route (0.0.0.0/0) points out port2.

The matching firewall policy denies the traffic → The log line Denied by forward policy check (policy 2) confirms that policy 2 matched and explicitly dropped the traffic.

NEW QUESTION: 71

An administrator wanted to configure an IPS sensor to block traffic that triggers a signature set number of times during a specific time period.

How can the administrator achieve the objective?

- A. Use IPS group signatures, set rate-mode 60.
- B. Use IPS packet logging option with periodical filter option.
- C. Use IPS filter, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

Answer: C ([LEAVE A REPLY](#))

The IPS filter with the rate-mode set to "periodical" allows the administrator to block traffic that triggers a signature a specified number of times within a defined time period, meeting the requirement.

NEW QUESTION: 72

Refer to the exhibits.

Antivirus profile

Edit AntiVirus Profile

Name

Comments 0/255

AntiVirus scan ☒ **Block** Monitor

Feature set **Proxy-based**

Inspected Protocols

HTTP	☒
SMTP	☐
POP3	☐
IMAP	☐
FTP	☒
CIFS	☐
MAPI	☐
SSH	☐

Firewall policy

Edit Policy

Incoming interface

Outgoing interface

Source & Destination

Source

User/group

Destination

Service

Firewall/Network Options

Inspection mode ☐ ☒

NAT ☒

IP pool configuration ☒ ☐

Preserve source port ☐

Protocol options ☒ ☐

Security Profiles

AntiVirus ☒ ☒ HTTP_AV_Profile

Web filter ☐

Video filter ☐

DNS filter ☐

Application control ☐

IPS ☐

File filter ☐

SSL inspection ☒ certificate-inspection



HTTPS access

FORTINET®



You are asked to implement an antivirus profile for files downloaded through FTP, HTTP, and HTTPS.

While testing, you are successful with HTTP and FTP protocols, but FortiGate does not block the file download over HTTPS.

What could be the cause?

- A. The feature set in the antivirus profile is not set to Flow-based.
- B. Web filter is not enabled on the firewall policy to complement the antivirus profile.
- C. The action on the firewall policy is not set to deny.
- D. The SSL inspection mode in the firewall policy is not deep content inspection.

Answer: ([SHOW ANSWER](#))

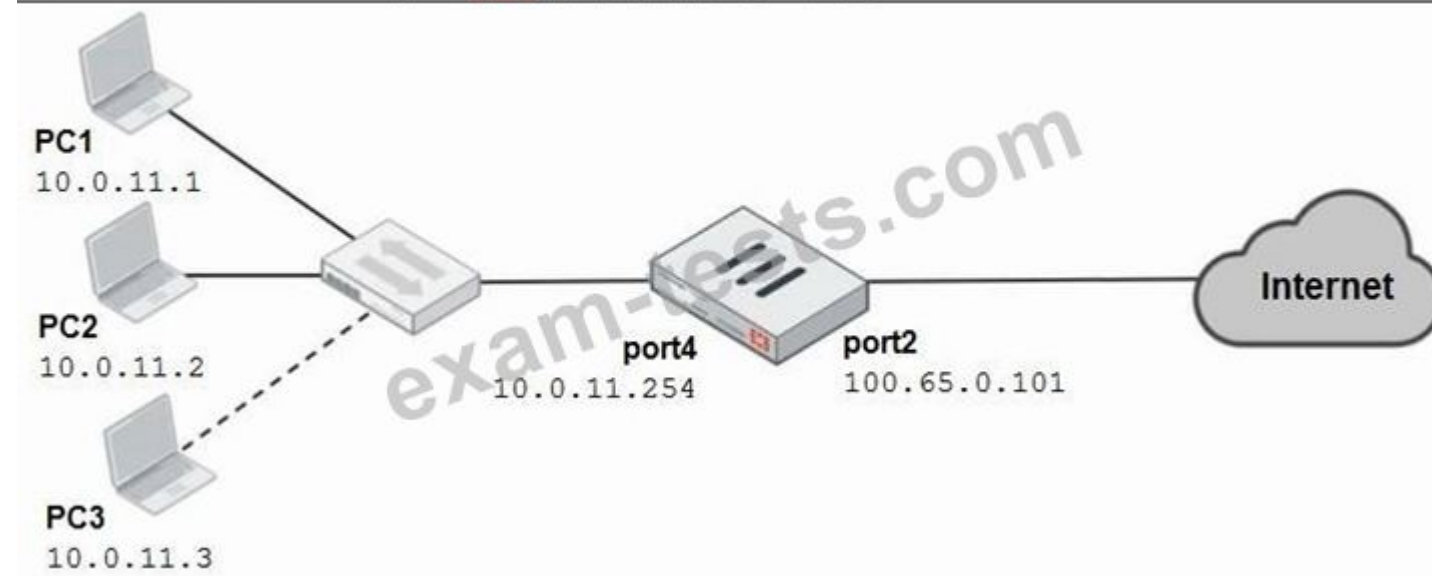
The SSL inspection mode in the firewall policy is set to certificate-inspection, which only examines SSL certificates without decrypting HTTPS traffic. Because of this, FortiGate cannot inspect or block files downloaded over HTTPS, as the content remains encrypted. To enable antivirus scanning on HTTPS traffic, the SSL inspection mode must be set to deep-inspection, allowing the FortiGate to decrypt, inspect, and re-encrypt the traffic.

NEW QUESTION: 73

Refer to the exhibits. The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device.

Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet.

Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)



Dynamic IP pool

Edit Dynamic IP Pool

Name	Internet-pool
Comments	Write a comment... 0/255
Type	One-to-One
External IP Range	100.65.0.110-100.65.0.111
ARP Reply	☒

Firewall policies

Edit Policy

Name ⓘ

Schedule  always ▼

Action ☒ ACCEPT ☐ DENY

Incoming interface  LAN(port4) ×
+

Outgoing interface  WAN(port2) ×
+

Source & Destination

Show logic

Source  all ×
+

User/group
+

Destination  all ×
+

Service  ALL ×
+

Firewall/Network Options

Inspection mode ☐ Flow-based ☒ Proxy-based

NAT ☒

IP pool configuration ☐ Use Outgoing Interface Address ☒ Use Dynamic IP Pool
 Internet-pool ×
+

Preserve source port ☐

Protocol options ☒ PROT default ▼

- A. In the IP pool configuration, set type to overload.
- B. In the system settings, set Multiple Interface Policies to enable.

C. In the firewall policy, set match-vipto enable using CLI.

D. In the IP pool configuration, set endip to 100.65.0.112.

Answer: ([SHOW ANSWER](#))

The IP pool is configured as One-to-One with a range of only 100.65.0.110-100.65.0.111, which allows NAT for only two internal hosts (PC1 and PC2). When PC3 tries to access the internet, no external IP is available for mapping.

To fix this:

- Change the IP pool type to Overload, allowing multiple internal IPs to share a single external IP.
- Expand the IP pool range by setting endip to 100.65.0.112 (or more) so that additional internal hosts (like PC3) can also be assigned a unique external IP.

NEW QUESTION: 74

Refer to the exhibit.

The screenshot shows the 'Edit Address' configuration window in Fortinet's management interface. The 'Name' field is set to 'Fortinet'. The 'Color' field has a 'Change' button next to it. The 'Interface' dropdown is set to 'port2'. The 'Type' dropdown is set to 'FQDN'. The 'FQDN' field contains 'www.fortinet.com'. The 'Routing configuration' toggle switch is currently turned off. The 'Comments' field has a placeholder text 'Write a comment...' and a character count '0/255'. A large, semi-transparent watermark 'exam-tests.com' is overlaid across the center of the form.

An administrator has created a new firewall address to use as the destination for a static route.

Why is the administrator not able to select the new address in the Destination field of the new static route?

- A.** In the new static route, the administrator must select Named Address.
- B.** In the new firewall address, the FQDN address must first be resolved.
- C.** In the new static route, the administrator must first set the interface to port2.
- D.** In the new firewall address, Routing configuration must be enabled.

Answer: D ([LEAVE A REPLY](#))

To use an FQDN-based address object as a destination in a static route, the "Routing configuration" option must be enabled in the firewall address settings. Without this, the address cannot be selected for routing.

NEW QUESTION: 75

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate.

Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

- A. Allow
- B. Trust & Allow
- C. Allow & Warning
- D. Block
- E. Block & Warning

Answer: ([SHOW ANSWER](#))

When FortiGate performs SSL/SSH full inspection, it can be configured to take one of several actions upon detecting an invalid certificate:

Allow → Lets the traffic through without restriction.

Allow & Warning → Permits the traffic but warns the user about the certificate issue.

Block → Denies the traffic outright to prevent insecure connections.

NEW QUESTION: 76

An administrator manages a FortiGate model that supports NTurbo.

How does NTurbo acceleration enhance antivirus performance?

- A. For proxy-based inspection, NTurbo offloads traffic to the content processor.
- B. For flow-based inspection, NTurbo establishes a dedicated data path to redirect traffic between the IPS engine and FortiGate ingress and egress interfaces.
- C. For proxy-based inspection, NTurbo buffers the whole file and then sends it to the antivirus engine.
- D. For flow-based inspection, NTurbo creates two inspection sessions on the FortiGate device.

Answer: B ([LEAVE A REPLY](#))

With flow-based inspection, NTurbo improves antivirus performance by establishing a dedicated fast data path that redirects traffic between the IPS engine and the FortiGate ingress/egress interfaces. This reduces CPU overhead, allowing antivirus scanning to happen at higher throughput without requiring full proxy-based buffering.

Valid FCP_FGT_AD-7.6 Dumps shared by BraindumpsPass.com for Helping Passing FCP_FGT_AD-7.6 Exam! BraindumpsPass.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the BraindumpsPass.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com FCP_FGT_AD-7.6 dumps with Test Engine here: https://www.braindumpspass.com/Fortinet/FCP_FGT_AD-7.6-practice-exam-dumps.html (132 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 77

Refer to the exhibit. What would be the impact of these settings on the Server certificate SNI check configuration on FortiGate?

Edit SSL/SSH Inspection Profile

FORTINET

Protecting SSL Server

Inspection method: SSL Certificate Inspection **Full SSL Inspection**

CA certificate: Fortinet_CA_SSL [Download](#)

Blocked certificates: [Allow](#) **Block** [View Blocked Certificates](#)

Untrusted SSL certificates: [Allow](#) **Block** [Ignore](#) [View Trusted CAs List](#)

Server certificate SNI check: [Enable](#) **Strict** [Disable](#)

- A. FortiGate will accept and use the CN in the server certificate for URL filtering if the SNI does not match the CN or SAN fields.
- B. FortiGate will accept the connection with a warning if the SNI does not match the CN or SAN fields.
- C. FortiGate will close the connection if the SNI does not match the CN or SAN fields.
- D. FortiGate will close the connection if the SNI does not match the CN and SAN fields

Answer: D (LEAVE A REPLY)

With the Server certificate SNI check set to Strict, FortiGate enforces that the SNI must match either the Common Name (CN) or Subject Alternative Name (SAN) in the server certificate; otherwise, it closes the connection.

NEW QUESTION: 78

An administrator manages a FortiGate model that supports NTurbo.

How does NTurbo enhance performance for flow-based inspection?

- A. NTurbo buffers the whole file and then sends it to the antivirus engine.
- B. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.
- C. NTurbo creates two inspection sessions on the FortiGate device.
- D. NTurbo offloads traffic to the content processor.

Answer: B (LEAVE A REPLY)

NTurbo enhances flow-based inspection performance by creating a fast data path between the IPS engine and the ingress/egress interfaces. This allows traffic to be inspected efficiently without needing to pass through the slower, traditional packet path, thus reducing CPU load and improving throughput during flow-based security inspections.

NEW QUESTION: 79

Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Firewall policy configuration

Edit Policy

Name	Internet_Access		
Incoming Interface	port2	+	✕
Outgoing Interface	port1	+	✕
Source	all	+	✕
Destination	all	+	✕
Schedule	always		
Service	DNS ✕ FTP ✕ HTTP ✕ HTTPS ✕		
Action	☒ ACCEPT ☐ DENY		
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	☒ PROE default		
Security Profiles			
AntiVirus	☒	default	
Web Filter	☐		
DNS Filter	☐		
Application Control	☐		
IPS	☐		
File Filter	☐		
SSL Inspection		deep-inspection	

Antivirus profile configuration

Edit AntiVirus Profile

Name default

Comments Scan files and block viruses. 29/255

AntiVirus scan   **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  

Send files to FortiSandbox for inspection  

Send files to FortiNDR for inspection  

Include mobile malware protection 

Quarantine  

Virus Outbreak Prevention

Use FortiGuard outbreak prevention database 

Use external malware block list 

Use EMS threat feed  

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

- A. Flow-based inspection is used, which resets the last packet to the user.
- B. The option to send files to FortiSandbox for inspection is enabled.
- C. The firewall policy performs a full content inspection on the file.
- D. The intrusion prevention security profile must be enabled when using flow-based inspection mode.

Answer: A (LEAVE A REPLY)

When flow-based inspection is used, FortiGate scans packets as they flow through, and if a virus is detected, the connection is reset immediately. Because the infected file is blocked mid-transfer, the user does not receive a block replacement message - only the last packet is dropped to terminate the connection.

Replacement messages are shown only in proxy-based inspection, where FortiGate can buffer and fully analyze the file before sending a response page.

Valid FCP_FGT_AD-7.6 Dumps shared by BraindumpsPass.com for Helping Passing FCP_FGT_AD-7.6 Exam! BraindumpsPass.com now offer the **newest FCP_FGT_AD-7.6 exam dumps**, the BraindumpsPass.com FCP_FGT_AD-7.6 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com FCP_FGT_AD-7.6 dumps with Test Engine here: https://www.braindumpsPass.com/Fortinet/FCP_FGT_AD-7.6-practice-exam-dumps.html (132 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)