

Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1

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?

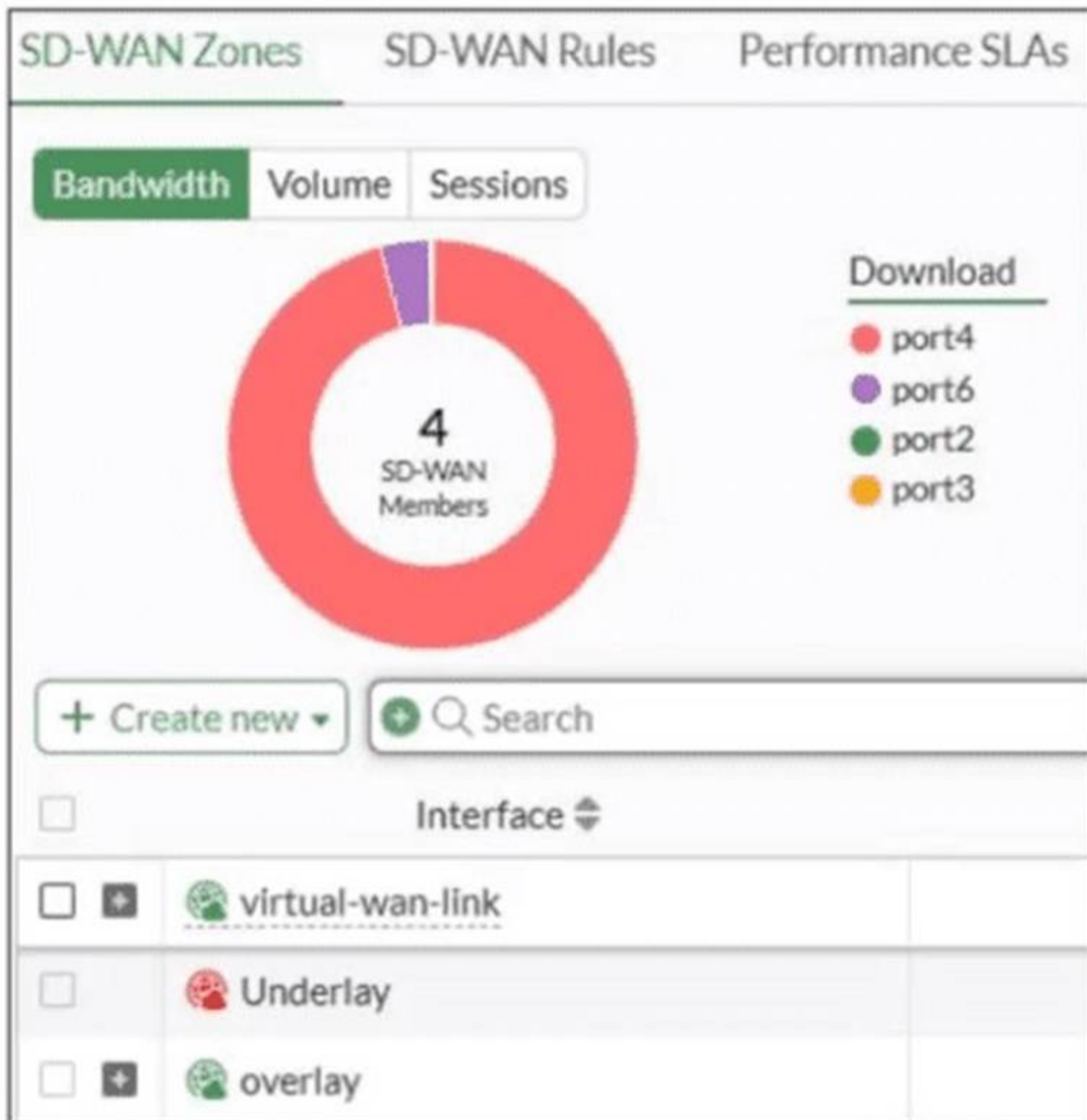
- A. By Sequence View groups policies based on rule priority, while Interface Pair View always follows the order of traffic logs.
- B. The firewall dynamically reorders policies in Interface Pair View based on recent traffic patterns, but By Sequence View remains static.
- C. Interface Pair View sorts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

Answer: C

NEW QUESTION 2

Refer to the exhibit.

FortiGate SD-WAN zone configuration



An SD-WAN zone configuration on the FortiGate GUI is shown. Based on the exhibit, which statement is true?

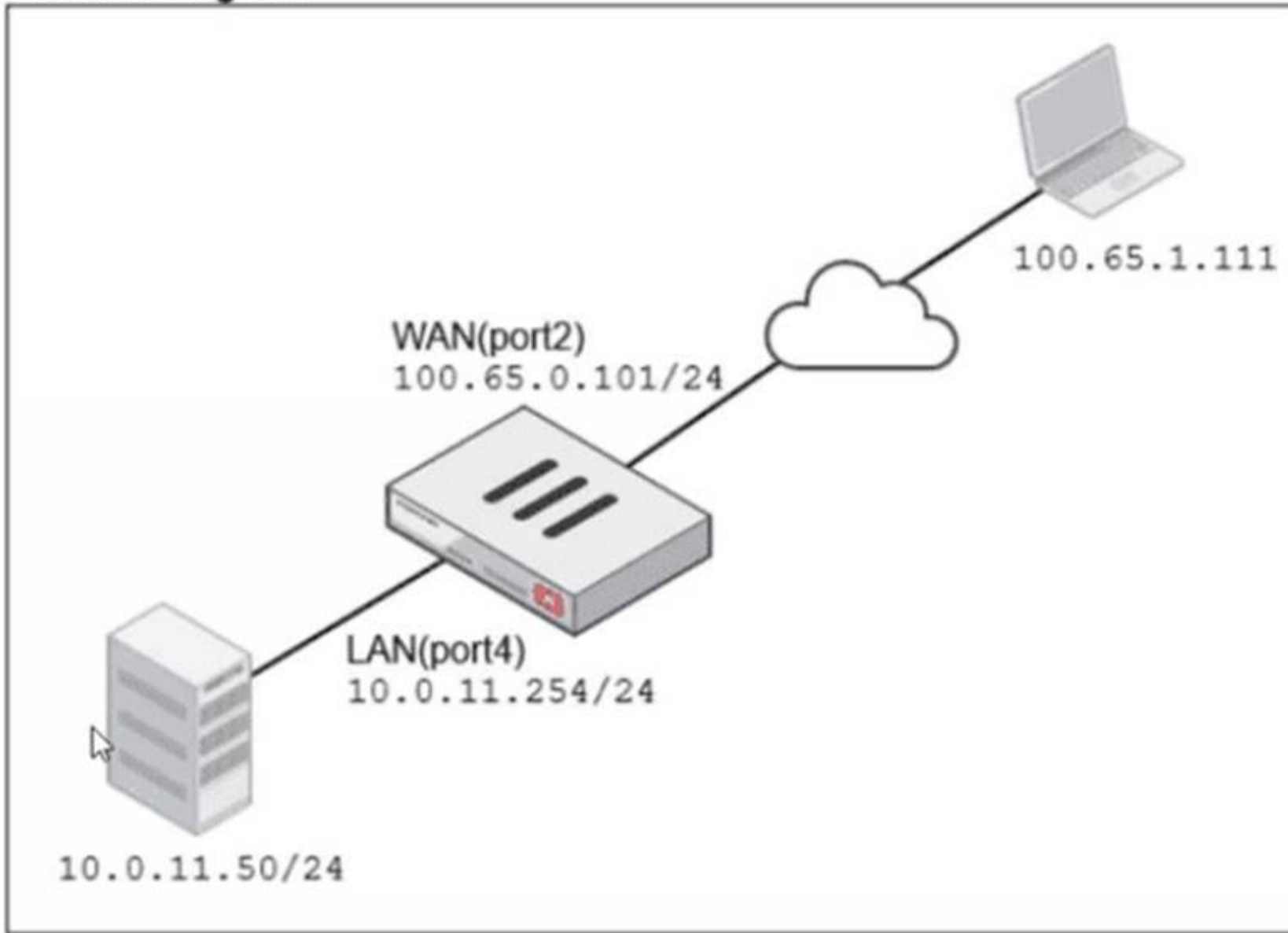
- A. The Underlay zone contains no member.
- B. The virtual-wan-link and overlay zones can be deleted
- C. The Underlay zone is the zone by default.
- D. port2 and port3 are not assigned to a zone.

Answer: A

NEW QUESTION 3

Refer to the exhibits.

Network diagram



Name: VIP-WEB-SERVER

Comments: Write a comment... 0/255

Color: Change

Network

Interface: WAN (port2)

Type: Static NAT

External IP address/range: 100.65.0.200

Map to:

IPv4 address/range: 10.0.11.50

Optional Filters

Port Forwarding

Protocol: TCP UDP SCTP ICMP

Port Mapping Type: One to one Many to many

External service port: 443

Map to IPv4 port: 4443

Firewall policies

Policy	From	To	Source	Destination	Schedule	Service	Action	IP Pool	NAT
<input type="checkbox"/> Internet (1)	LAN (port4)	WAN (port2)	all	all	always	ALL	<input checked="" type="checkbox"/> ACCEPT		<input checked="" type="checkbox"/> NAT
<input type="checkbox"/> Web_Server_Access (2)	WAN (port2)	LAN (port4)	all	VIP-WEB-SERVER	always	HTTPS	<input checked="" type="checkbox"/> ACCEPT		<input checked="" type="checkbox"/> Disabled

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 100.65.1.111 sends 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?

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

Answer: C

NEW QUESTION 4

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. Enabled
- C. On Idle
- D. Usabled

Answer: A

NEW QUESTION 5

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

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

Answer: BC

NEW QUESTION 6

Refer to the exhibit.

Profile Name ↕
Monitoring_Access
NOC_Access
prof_admin
super_admin

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? (Choose one answer)

- 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: D

NEW QUESTION 7

Refer to the exhibit.

A RADIUS server configuration is shown.

New RADIUS Server

Name

Authentication method Default Specify

NAS IP

Include in every user group

Primary Server

IP/Name

Secret

An administrator added a configuration for a new RADIUS server. While configuring, the administrator enabled "Include in every user group". What is the impact of enabling "Include in every user group" in a RADIUS configuration?

- A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
- B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
- C. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.
- D. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.

Answer: A

NEW QUESTION 8

An administrator manages a FortiGate model that supports NTurbo. How does NTurbo acceleration enhance antivirus performance?

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

Answer: A

NEW QUESTION 9

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 system performance output and default configuration of high memory usage thresholds on a FortiGate device are shown. Based on the system performance output, what are the two possible outcomes? (Choose two.)

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

Answer: BD

NEW QUESTION 10

Refer to the exhibit.

```
HQ-NGFW-1 # diagnose test application ipsmonitor 1
pid = 2044, engine count = 0 (+1)
0 - pid:2074:2074 cfg:1 master:0 run:1
```

As an administrator you have created an IPS profile, but it is not performing as expected. While testing you got the output as shown in the exhibit. What could be the possible reason of the diagnose output shown in the exhibit?

- A. There is a no firewall policy configured with an IPS security profile.
- B. Administrator entered the command diagnose test application ipsmonitor 5.
- C. FortiGate entered into IPS fail open state.
- D. Administrator entered the command diagnose test application ipsmonitor 99.

Answer: A

NEW QUESTION 10

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

Answer: A

NEW QUESTION 14

FortiGate is integrated with FortiAnalyzer and FortiManager.

When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

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

Answer: A

NEW QUESTION 16

Refer to the exhibits.

Application sensor

Edit Application Sensor

Categories

Mixed ▾ All Categories

Business (157, 6)

Cloud/IT (72, 12)

Collaboration (266, 13)

Email (76, 11)

Game (83)

General Interest (254, 15)

Mobile (3)

Network Service (338)

Operational Technology

P2P (55)

Proxy (189)

Remote Access (96)

Social Media (113, 29)

Storage/Backup (150, 20)

Update (48)

Video/Audio (148, 17)

VoIP (23)

Web Client (24)

Unknown Applications

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

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:

Video filter:

DNS filter:

Application control: APP default

IPS:

File filter:

SSL inspection: SSL certificate-inspection

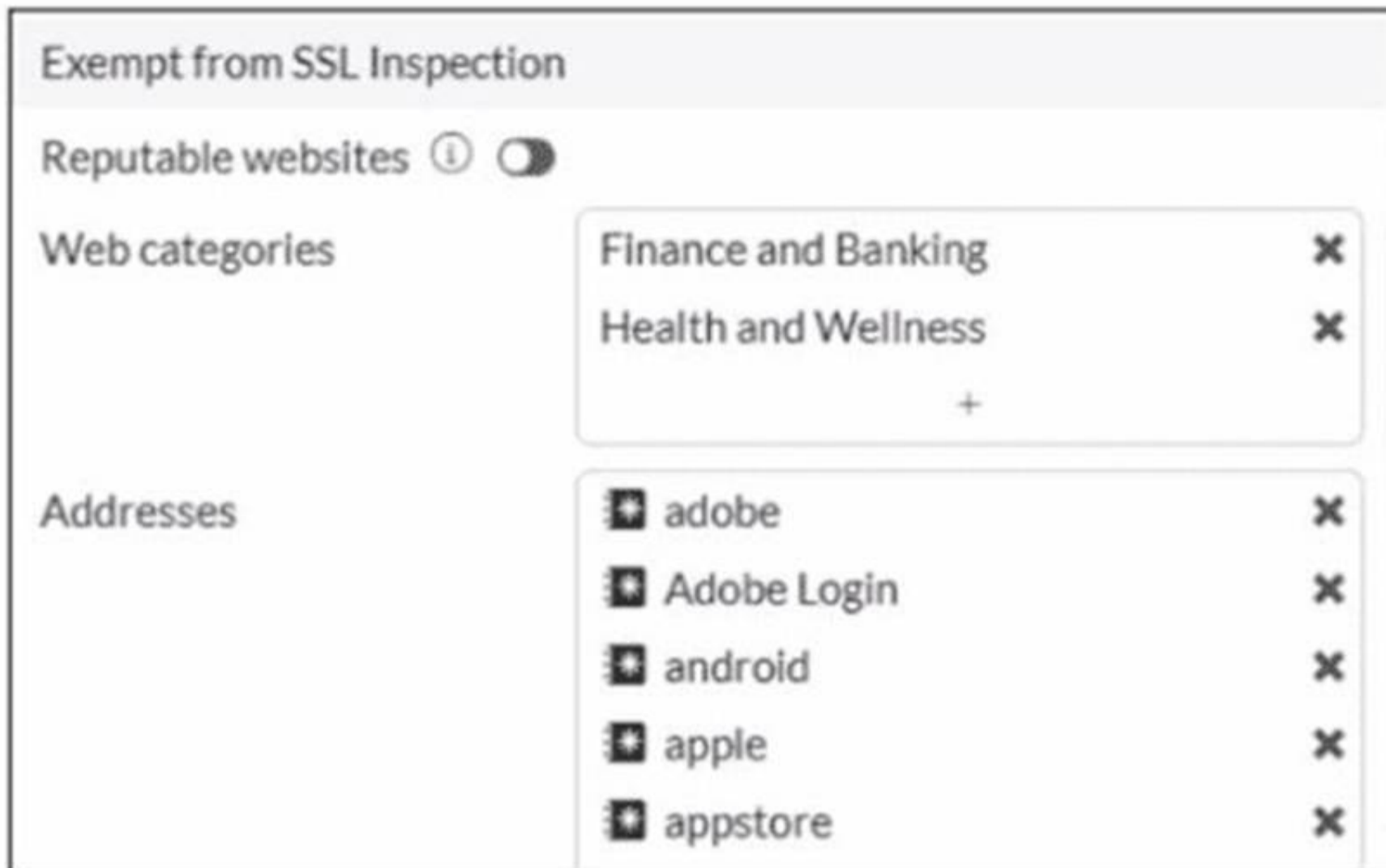
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. Which two actions would you take to resolve the issue? (Choose two.)

- A. Set SSL inspection to deep-content inspection.
- B. Move up Google in the Application and Filter Overrides section to set its priority lot
- C. Add "Google".com to the URL category in the security profile.
- D. Change the Inspection mode to Flow-based
- E. Set the action for Google in the Application and Filter Overrides section to Allow

Answer: BE

NEW QUESTION 17

Refer to the exhibit.



The predefined deep-inspection and custom-deep-inspection profiles exclude some web categories from SSL inspection, as shown in the exhibit For which two reasons are these web categories exempted? (Choose two.)

- A. The resources utilization is optimized because these websites are in the trusted domain list on FortiGate.
- B. The legal regulation aims to prioritize user privacy and protect sensitive information for these websites.
- C. These websites are in an allowlist of reputable domain names maintained by FortiGuard.
- D. The FortiGate temporary certificate denies the browser's access to websites that use HTTP Strict Transport Security.

Answer: BC

NEW QUESTION 22

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

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

Answer: CDE

NEW QUESTION 26

An administrator wanted to configure an IPS sensor to block traffic that triggers the 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 signatures, rate-mode periodical option.
- D. Use IPS filter, rate-mode periodical option.

Answer: D

NEW QUESTION 29

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

Answer: D

NEW QUESTION 34

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

Answer: CD

NEW QUESTION 35

Refer to the exhibit.

SD-WAN traffic log

Application Name	Result	Policy ID	Destination Interface	SD-WAN Quality	SD-WAN Rule Name
YouTube	✓ Accept (8.08 kB / 27...)	1 (DIA)	port2		
YouTube	✓ Accept (UTM Allowed)	1 (DIA)	port2		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (UTM Allowed)	1 (DIA)	port1		
Facebook	✓ Accept (3.33 kB / 10...)	1 (DIA)	port1		
YouTube	✓ Accept (44.63 kB / 3...)	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port1		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		
CNN	✓ Accept (UTM Allowed)	1 (DIA)	port2		

The administrator configured SD-WAN rules and set the FortiGate traffic log page to display SD-WAN-specific columns: SD-WAN Quality and SD-WAN Rule Name. FortiGate allows the traffic according to policy ID 1 placed at the top. This is the policy that allows SD-WAN traffic. Despite these settings, the traffic logs do not show the name of the SD-WAN rule used to steer those traffic flows. What could be the reason?

- A. SD-WAN rule names do not appear immediately.
- B. The administrator must refresh the page.
- C. There is no application control profile applied to the firewall policy.
- D. Destinations in the SD-WAN rules are configured for each application, but feature visibility is not enabled.
- E. FortiGate load balanced the traffic according to the implicit SD-WAN rule.

Answer: D

NEW QUESTION 39

What are two features of collector agent advanced mode? (Choose two.)

- A. In advanced mode, security profiles can be applied only to user groups, not individual users.
- B. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
- C. Advanced mode uses the Windows convention—NetBios: Domain\Username.
- D. Advanced mode supports nested or inherited groups.

Answer: BD

NEW QUESTION 43

An administrator has configured a dialup IPsec VPN on FortiGate with add-route enabled. However, the static route is not showing in the routing table. Which two statements about this scenario are correct? (Choose two.)

- A. The administrator must use a policy route instead of a static route for add-route to work properly.
- B. The administrator must ensure phase 2 is successfully established.
- C. The administrator must define the remote network correctly in the phase 2 selectors.
- D. The administrator must enable a dynamic routing protocol on the dialup interface.

Answer: BC

NEW QUESTION 44

When configuring firewall policies which of the following is true regarding the policy ID? (Choose two.)

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

Answer: BC

NEW QUESTION 49

Refer to the exhibit.

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" euid=3 epid=3 dsteuid=3 dstepid=101
logflag=0 logver=706003401 type="utm" subtype="app-ctrl" level="warning" action="block" sessionid=510 policyid=1 srcip=
10.0.11.50 dstip=54.146.230.62 srcport=53398 dstport=80 proto=6 logid=1059028705 service="HTTP" eventtime=
1756915797391471958 incidentserialno=116391982 direction="outgoing" apprisk="elevated" appid=30220 srcintfrole="undefined"
dstintfrole="undefined" applist="default" appcat="Video/Audio" app="ABC.Com" hostname="abc.go.com" url="/favicon.ico"
eventtype="signature" srcintf="port4" dstintf="port2" msg="Video/Audio: ABC.Com" tz="-0700" policytype="policy"
srccountry="Reserved" dstcountry="United States" poluid="b11ac58c-791b-51e7-4600-12f829a689d9" agent="Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:142.0) Gecko/20100101 Firefox/142.0" httpmethod="GET" referralurl="http://abc.go.com/"
devid="FGVM02TM24013423" vd="root" dtime="2025-09-03 09:09:57" itime_t=1756915802 devname="HQ-NGFW-1"
```

Which two ways can you view the log messages shown in the exhibit? (Choose two.)

- A. By right clicking the implicit deny policy
- B. Using the FortiGate CLI command diagnose log test
- C. By filtering by policy universally unique identifier (UUID) and application name in the log entry
- D. In the Forward Traffic section

Answer: CD

NEW QUESTION 51

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

Answer: CD

NEW QUESTION 53

Refer to the exhibits.

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	<input checked="" type="radio"/> Allow
Medicine	<input checked="" type="radio"/> Allow
News and Media	<input checked="" type="radio"/> Allow
Social Networking	<input checked="" type="radio"/> Allow
Political Organizations	<input checked="" type="radio"/> Allow
Reference	<input checked="" type="radio"/> Allow
Global Religion	<input checked="" type="radio"/> Allow
Shopping	<input checked="" type="radio"/> Allow
Society and Lifestyles	<input checked="" type="radio"/> 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	<input type="radio"/> Monitor	<input checked="" type="radio"/> 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: PROT default

Security Profiles

AntiVirus:

Web filter: WEB default

Video filter:

DNS filter:

Application control:

IPS:

File filter:

SSL inspection: SSL certificate-inspection

FortiGuard block page



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?

- A. The web rating override configuration is incorrect.
- B. The web filter profile feature set is configured incorrectly.
- C. The firewall policy inspection mode is incorrect.
- D. For ww
- E. faceboo
- F. co
- G. the URL filter action is incorrect.

Answer: C

NEW QUESTION 58

Refer to the exhibit.
 A routing table is shown

Network	Gateway IP	Interfaces	Distance	Metric	Priority	Type
10.0.11.0/24	0.0.0.0	port4	0	0	0	Connected
10.0.12.0/24	0.0.0.0	port5	0	0	0	Connected
10.0.13.0/24	0.0.0.0	port6	0	0	0	Connected
100.65.0.0/24	0.0.0.0	port2	0	0	0	Connected
100.66.0.0/24	0.0.0.0	port3	0	0	0	Connected
172.20.1.0/24	100.66.0.254	port3	9	0	2	Static
192.168.0.0/16	0.0.0.0	port1	0	0	0	Connected

An administrator wants to create a new static route so the traffic to the subnet 172.20.1.0/24 is routed through port2 only. What are the two criteria that the administrator can use to achieve this objective? (Choose two.)

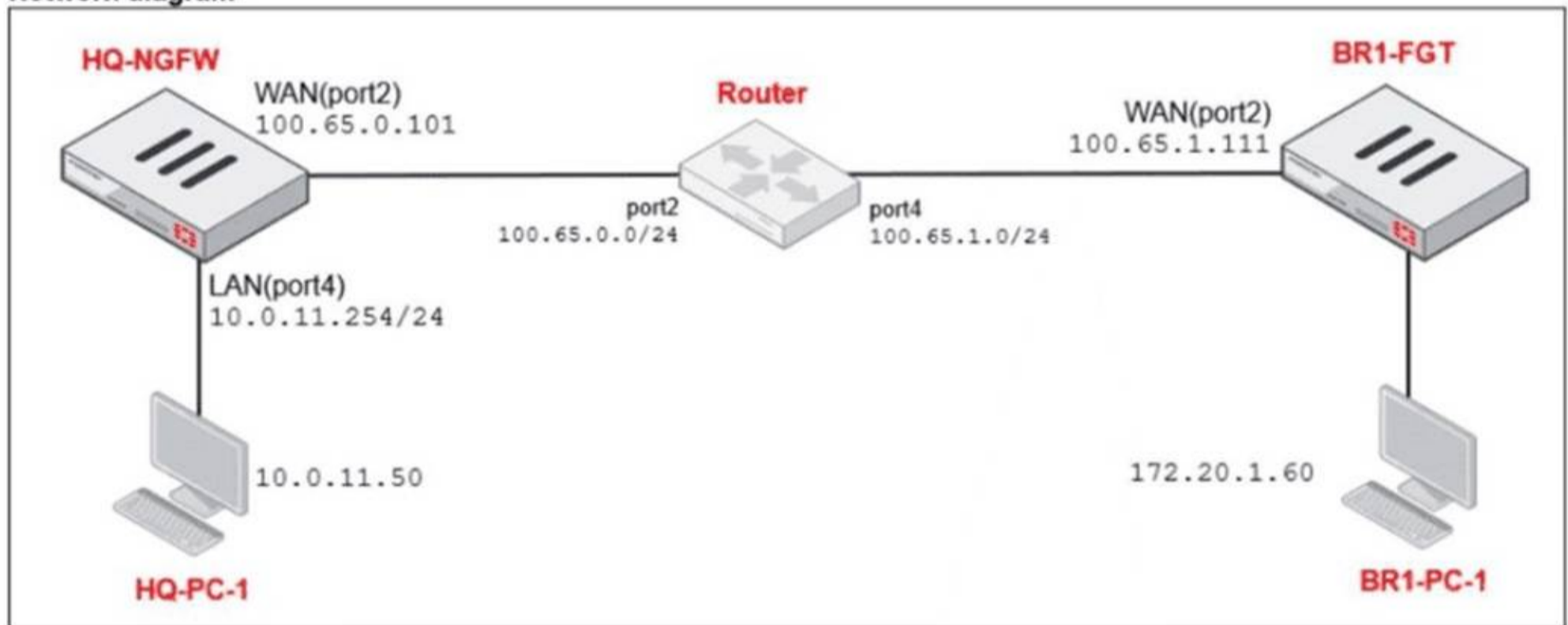
- A. The new static route must have the priority set to 3.
- B. The new static route must have the metric set to 1.
- C. The existing static route through port3 must have the distance set to 11.
- D. The new static route must have the distance set to 9

Answer: CD

NEW QUESTION 60

Refer to the exhibits.

Network diagram



NAT IP pool configuration

<input type="checkbox"/>	Name	External IP Range	Type	ARP Reply
<input type="checkbox"/>	SNAT-Pool	100.65.0.49 - 100.65.0.49	Overload	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/>	SNAT-Remote	100.65.0.149 - 100.65.0.149	Overload	<input checked="" type="checkbox"/> Enabled
<input type="checkbox"/>	SNAT-Remote1	100.65.0.99 - 100.65.0.99	Overload	<input checked="" type="checkbox"/> Enabled

Firewall policies

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT
LAN (port4) → WAN (port2) 3							
<input type="checkbox"/>	TCP traffic (2)	all	BR1-FGT	always	ALL_TCP	ACCEPT	SNAT-Pool NAT
<input type="checkbox"/>	PING traffic (3)	all	all	always	PING	ACCEPT	SNAT-Remote1 NAT
<input type="checkbox"/>	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. 100.65.0.149
- D. 100.65.0.99

Answer: D

NEW QUESTION 61

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

NSE4_FGT_AD-7.6 Practice Exam Features:

- * NSE4_FGT_AD-7.6 Questions and Answers Updated Frequently
- * NSE4_FGT_AD-7.6 Practice Questions Verified by Expert Senior Certified Staff
- * NSE4_FGT_AD-7.6 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE4_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE4_FGT_AD-7.6 Practice Test Here](#)