

Fortinet

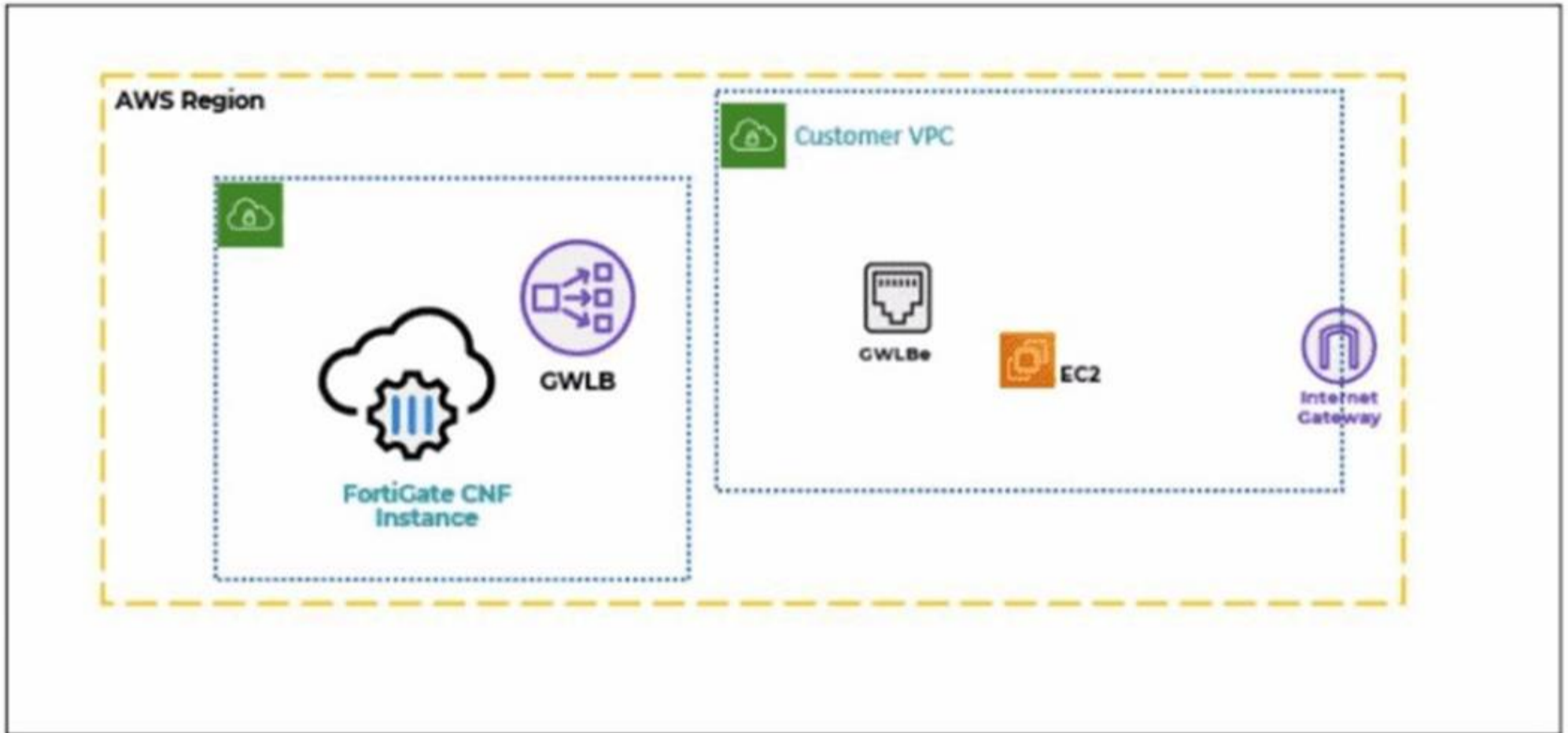
Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1

Refer to the exhibit.
 A partial cloud topology is shown.



You deployed a FortiGate Cloud-Native Firewall (CNF) in AWS.
 During the deployment, which components must the FortiGate CNF create to handle traffic from the EC2 instance?

- A. The customer VPC and GWLB
- B. The gateway load balancer endpoint (GWLBe) in the customer virtual private cloud (VPC)
- C. The CNF VP
- D. customer VP
- E. and GWLB
- F. The GWL
- G. GWLBe, and the internet gateway (IGW) in the customer VPC

Answer: B

NEW QUESTION 2

Refer to the exhibit.

Application and Filter Overrides			
Priority	Details	Type	Action
1	ABC.Com	Application	<input checked="" type="checkbox"/> Allow
2	Excessive-Bandwidth	Filter	<input type="checkbox"/> 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 is hitting the category Excessive-Bandwidth.
- B. The ABC.Com Type is set as Application instead of Filter.
- C. The ABC.Com is configured under application profile, which must be configured as a web filter profile.
- D. The ABC Com Action is set to Allow

Answer: D

NEW QUESTION 3

Refer to the exhibit.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-filter
Status      : Enable
License     : Contract
\
Num. of servers : 1
Protocol    : https
Port        : 8888
Anycast     : Disable
Default servers : Not included

--- Server List (Wed Sep 20 09:22:42 2023) ---

IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr Lost  Total Lost  Updated Time
10.0.1.241   -244    2 I    0    122                0          0  Wed Sep 20 09:21:55 2023
```

Which two statements about the FortiGuard connection are true? (Choose two.)

- A. The weight increases as the number of failed packets rises
- B. You can configure unreliable protocols to communicate with FortiGuard Server.
- C. FortiGate identified the FortiGuard Server using DNS lookup.
- D. FortiGate is using the default port for FortiGuard communication.

Answer: AD

NEW QUESTION 4

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-fffffffa002c9c7

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 iprope_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 answers)

- 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: AD

NEW QUESTION 5

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
```

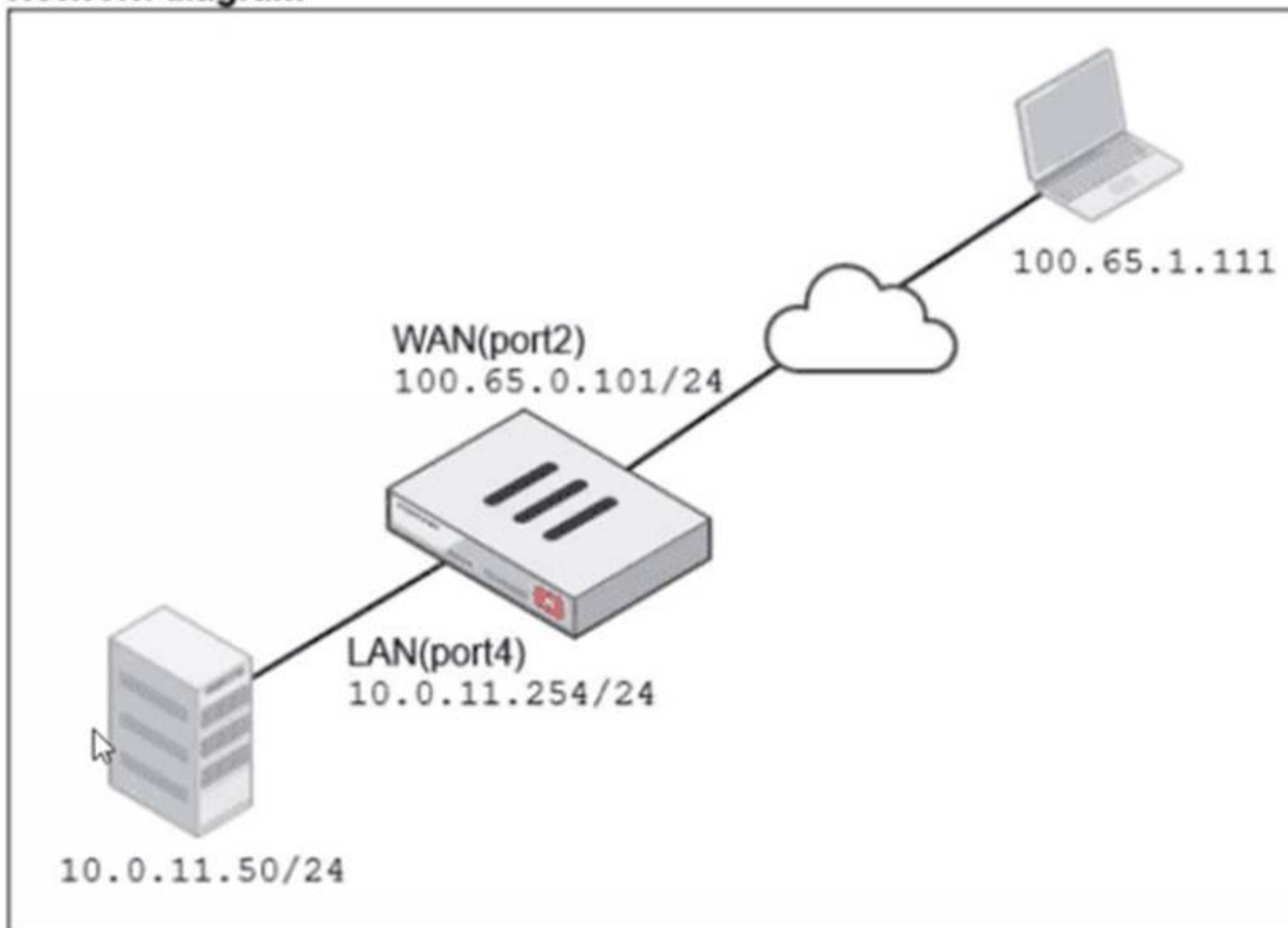
What would be the impact of this configuration on FortiGate?

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

Answer: A


NEW QUESTION 6
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 7

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? (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 8

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. Network Protocol Enforcement
- C. Replacement Messages for UDP-based Applications
- D. Application and Filter Overrides

Answer: B

NEW QUESTION 9

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

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

Answer: A

NEW QUESTION 10

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

- 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: CD

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 14

Refer to the exhibit.

IPsec tunnel configuration

The diagram shows two FortiGate devices, HQ-NGFW and BR1-FGT, connected via an IPsec tunnel. Below the diagram are two screenshots of the FortiGate configuration interface for Phase 2 selectors.

Left Screenshot (HQ-NGFW):

- Phase 2 selectors:** Table with columns Name, Local Address, Remote Address, Comments. Row: ToBR1, 10.0.11.0/255.255.255.0, 172.20.1.0/255.255.255.0.
- Edit Phase 2 Selector:** Name: ToBR1. Encapsulation: Tunnel Mode. IP version: IPv4. Remote address: 172.20.1.0 255.255.255.0.
- Advanced:** Encryption - authentication: AES128 - SHA1. Replay detection: Enable. Perfect forward secrecy (PFS): Enable. Diffie-Hellman groups: 5 (checked). Local port: All. Remote port: All. Protocol: All. Auto-negotiate: Enable. Autokey keep alive: Enable. Key lifetime: 43200 second(s).

Right Screenshot (BR1-FGT):

- Phase 2 selectors:** Table with columns Name, Local Address, Remote Address, Comments. Row: ToHQ, 172.20.1.0/255.255.255.0, 10.11.0.0/255.255.255.0.
- Edit Phase 2 Selector:** Name: ToHQ. Encapsulation: Tunnel Mode. IP version: IPv4. Remote address: 10.11.0.0 255.255.255.0.
- Advanced:** Encryption - authentication: AES256 - SHA1. Replay detection: Enable. Perfect forward secrecy (PFS): Enable. Diffie-Hellman groups: 14 (checked), 5 (checked). Local port: All. Remote port: All. Protocol: All. Auto-negotiate: Enable. Autokey keep alive: Enable. Key lifetime: 14400 second(s).

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 Remote Address to 10.0.11.0/255.255.255.0.
- B. On HQ-NGF
- C. enable Diffie-Hellman Group 2.
- D. On BR1-FG
- E. set Seconds to 43200
- F. On HQ-NGF
- G. set Encryption to AES256.

Answer: AD

NEW QUESTION 17

Which two components are part of the secure internet access (SIA) agent-based mode on FortiSASE? (Choose two.)

- A. FortiSASE Firewall-as-a-Service (FWaaS)
- B. The proxy auto-configuration (PAC) file
- C. VPN policies
- D. FortiExtender

Answer: AC

NEW QUESTION 18

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 21

Refer to the exhibits.

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 (31)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New
✎ Edit
🗑 Delete

Priority	Details	Type	Action
1	BIVR Excessive-Bandwidth	Filter	<input type="checkbox"/> Block
2	VEND Apple	Filter	<input checked="" type="checkbox"/> Monitor

Application override configuration

Edit Override

Type: Application Filter

Action: Block

Filter: BIVR Excessive-Bandwidth ✕

+

FaceTime ✕ 🔍

Name	Category	Technology
Application Signature 1/1262		
FaceTime	VoIP	Client-Server

Filter override configuration

Edit Override

Type: Application Filter

Action: Monitor

Filter: VEND Apple ✕

+

FaceTime ✕ 🔍

Name	Category	Technology
Application Signature 1/33		
FaceTime	VoIP	Client-Server

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? (Choose one answer)

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

Answer: B

NEW QUESTION 24

Which three statements explain a flow-based antivirus profile? (Choose three answers)

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

Answer: ABD

NEW QUESTION 25

Refer to the exhibits.

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	BHVR Excessive-Bandwidth	Filter	<input checked="" type="checkbox"/> Block
2	VEND Google	Filter	<input checked="" type="checkbox"/> 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:

DNS filter:

Application control: APP default

IPS:

File filter:

SSL inspection : SSL deep-inspection

Decrypted traffic mirror:

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

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

Answer: AB

NEW QUESTION 28

What is the primary FortiGate election process when the HA override setting is enabled? (Choose one answer)

- 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

NEW QUESTION 29

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 33

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

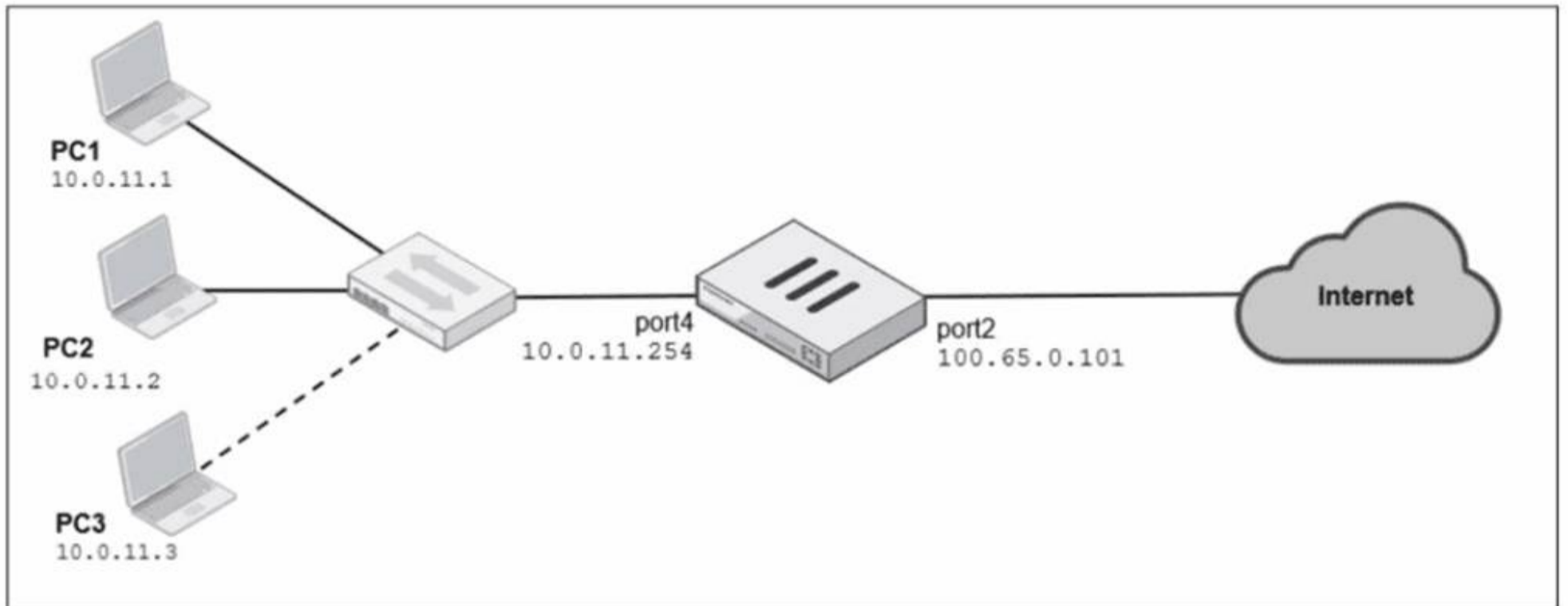
- A. In advanced mode, security profiles can be applied only to user groups, not individual users.
- B. In advanced mode, security profiles can be applied only to user groups, not individual users.
- C. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
-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

Answer: BD

NEW QUESTION 37

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 ⓘ	100.65.0.110-100.65.0.111
ARP Reply	<input type="checkbox"/>

Firewall policies

Edit Policy

Name (i)

Schedule

Action ACCEPT DENY

Outgoing interface ×

Source & Destination Show logic

Source ×

User/group +

Destination ×

Service ×

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 PROXY default

A diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device are shown. 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 system settings, set Multiple Interface Policies to enable.
- B. in the IP pool configuration, set end ip to 100.65.0.112.

- C. In the firewall policy, set match-vip to enable using CLI.
- D. In the IP pool configuration, set type to overload.

Answer: BD

NEW QUESTION 38

Refer to the exhibit.

```
date=2025-09-03 time=09:09:57 id=7545895911432388608 itime="2025-09-03 09:10:02" eid=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 41

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

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

Answer: B

NEW QUESTION 43

.....

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](#)