

Fortinet

Exam Questions NSE4_FGT_AD-7.6

Fortinet NSE 4 - FortiOS 7.6 Administrator



NEW QUESTION 1
Refer to the exhibit.

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

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 2
Which three strategies are valid SD-WAN rule strategies for member selection? (Choose three answers)

- A. Lowest Cost (SLA) without load balancing
- B. Manual with load balancing
- C. Lowest Quality (SLA) with load balancing
- D. Lowest Cost (SLA) with load balancing
- E. Best Quality with load balancing

Answer: ABD

NEW QUESTION 3
Refer to the exhibit.

IPsec tunnel configuration

The diagram illustrates the IPsec tunnel configuration between two FortiGate devices: HQ-NGFW and BR1-FGT. The HQ-NGFW configuration shows a Phase 2 selector named 'ToBR1' with Local Address 10.0.11.0/255.255.255.0 and Remote Address 172.20.1.0/255.255.255.0. The BR1-FGT configuration shows a Phase 2 selector named 'ToHQ' with Local Address 172.20.1.0/255.255.255.0 and Remote Address 10.11.0.0/255.255.255.0. Both configurations show advanced settings for encryption, authentication, and replay detection.

HQ-NGFW Phase 2 Selector Configuration:

- Name: ToBR1
- Local Address: 10.0.11.0/255.255.255.0
- Remote Address: 172.20.1.0/255.255.255.0
- Encapsulation: Tunnel Mode
- IP version: IPv4
- Named address: Disabled
- Remote address: Subnet Address (172.20.1.0 255.255.255.0)
- Encryption - authentication: AES128 - SHA1
- Replay detection: Enabled
- Perfect forward secrecy (PFS): Enabled
- Diffie-Hellman groups: 5 (selected)
- Local port: All
- Remote port: All
- Protocol: All
- Auto-negotiate: Enabled
- Autokey keep alive: Enabled
- Key lifetime: 43200 seconds

BR1-FGT Phase 2 Selector Configuration:

- Name: ToHQ
- Local Address: 172.20.1.0/255.255.255.0
- Remote Address: 10.11.0.0/255.255.255.0
- Encapsulation: Tunnel Mode
- IP version: IPv4
- Named address: Disabled
- Remote address: Subnet Address (10.11.0.0 255.255.255.0)
- Encryption - authentication: AES256 - SHA1
- Replay detection: Enabled
- Perfect forward secrecy (PFS): Enabled
- Diffie-Hellman groups: 14 (selected)
- Local port: All
- Remote port: All
- Protocol: All
- Auto-negotiate: Enabled
- Autokey keep alive: Enabled
- Key lifetime: 14400 seconds

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 4

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 5

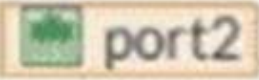
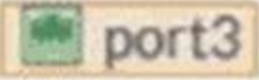
FortiGate is integrated with FortiAnalyzer and FortiManager.
When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

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

Answer: A

NEW QUESTION 6

Refer to the exhibit.

Destination ⇅	Gateway IP ⇅	Interface ⇅	Status ⇅
0.0.0.0/0	100.65.0.254	 port2	 Enabled
10.10.10.0/24	100.66.0.254	 port3	 Enabled
10.0.13.0/24	10.0.13.125	 port6	 Enabled

Based on the routing table shown in the exhibit, which two statements are true? (Choose two.)

- A. A packet with the source IP address 10.0.13.10 arriving on port2 is allowed if strict RPF is disabled.
- B. A packet with the source IP address 10.100.110.10 arriving on port2 is allowed if strict RPF is enabled.
- C. A packet with the source IP address 10.100.110.10 arriving on port3 is allowed if strict RPF is disabled.
- D. A packet with the source IP address 10.10.10.10 arriving on port2 is allowed if strict RPF is enabled.

Answer: AC

NEW QUESTION 7

Refer to the exhibit.

Edit SSL/SSH Inspection Profile

Inspection method

Protecting SSL Server

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

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: C

NEW QUESTION 8

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	BHVR Excessive-Bandwidth	Filter	Block
2	VEND Google	Filter	Monitor
2			

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

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

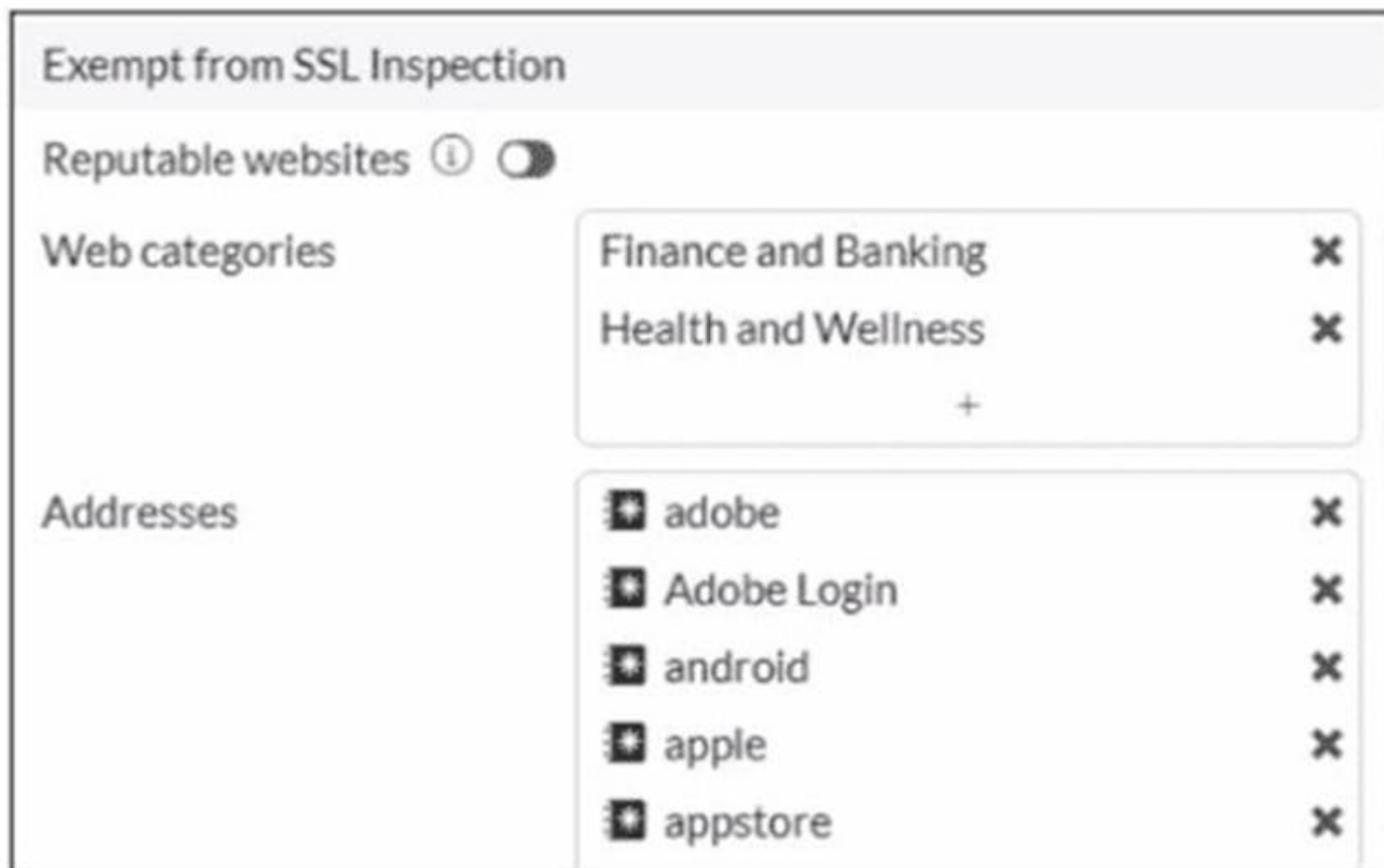
You have implemented the application sensor and the corresponding firewall policy as shown in the exhibits. You cannot access any of the Google applications, but you are able to access www.fortinet.com. Which two actions would you take to resolve the issue? (Choose two.)

- 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 9

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 10

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 10

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 12

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	 Block
2	VEND 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

☐

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 14

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 17

An administrator wants to form an HA cluster using the FGCP protocol.
Which two requirements must the administrator ensure both members fulfill? (Choose two.)

- A. They must have the same hard drive configuration.
- B. They must have the same number of configured VDOMs.
- C. They must have the heartbeat interfaces in the same subnet
- D. They must have the same HA group ID.

Answer: BD

NEW QUESTION 20

What are two characteristics of HA cluster heartbeat IP addresses in a FortiGate device? (Choose two.)

- A. Heartbeat IP addresses are used to distinguish between cluster members.
- B. The heartbeat interface of the primary device in the cluster is always assigned IP address 169.254.0.1.
- C. A change in the heartbeat IP address happens when a FortiGate device joins or leaves the cluster.
- D. Heartbeat interfaces have virtual IP addresses that are manually assigned.

Answer: AC

NEW QUESTION 22

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 25

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.
What is the reason for the certificate warning errors?

- A. The option invalid SSL certificates is set to allow on the SSL/SSH inspection profile.
- B. The matching firewall policy is set to proxy inspection mode.
- C. The browser does not trust the certificate used by FortiGate for SSL inspection.
- D. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

Answer: C

NEW QUESTION 27

How does FortiExtender connect to FortiSASE in a site-based, remote internet access method?

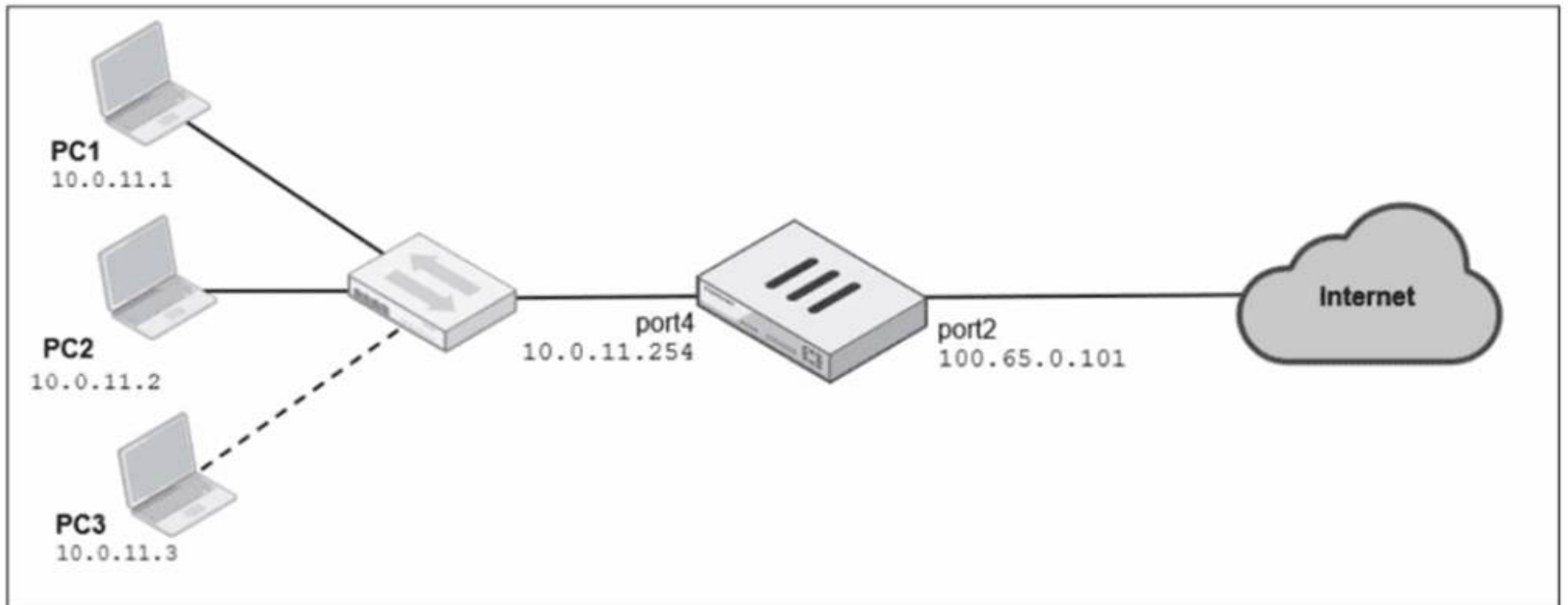
- A. FortiExtender uses a Virtual Extensible LAN (VXLAN)-over-IPsec connection.
- B. FortiExtender establishes a secure SSL connection using FortiClient.
- C. FortiExtender first connects to a FortiGate LAN extension through a secure web gateway (SWG).
- D. FortiExtender uses the proxy auto-configuration (PAC) file and an explicit web proxy to connect.

Answer: A

NEW QUESTION 30

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
☐

Firewall policies

Edit Policy

Name ⓘInternet

Schedulealways

✓ ACCEPT✗ DENY

Outgoing interfaceWAN (port2)

Source & DestinationShow logic

Sourceall

User/group

Destinationall

ServiceALL

Firewall/Network Options

Inspection modeFlow-basedProxy-based

NAT

IP pool configurationUse Outgoing Interface AddressUse Dynamic IP Pool

Internet-pool

Preserve source port

Protocol optionsPROTdefault

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.

Passing Certification Exams Made Easy

visit - <https://www.surepassexam.com>

- 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 33

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" poluuid="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 34

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 35

Refer to the exhibit

A firewall policy to enable active authentication is shown.

Policy	Source	Destination	Schedule	Service	Action	NAT	Type	Security Profiles
port4 → port2 1								
Internet (1)	HQ_SUBNET Remote-users	all	always	ALL_ICMP HTTPS HTTP	ACCEPT	NAT	Standard	Category_Monitor certificate-inspection

When attempting to access an external website using an active authentication method, the user is not presented with a login prompt. What is the most likely reason for this situation?

- A. No matching user account exists for this user.
- B. The Remote-users group must be set up correctly in the FSSO configuration.
- C. The Remote-users group is not added to the Destination
- D. The Service DNS is required in the firewall policy.

Answer: D

NEW QUESTION 39

Refer to the exhibits.

Web filter profile configuration

Edit Web Filter Profile

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

☒ FortiGuard Category Based Filter

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 ☒

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

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 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 First Try
- * NSE4_FGT_AD-7.6 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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