

# Fortinet

## Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)



#### NEW QUESTION 1

Which two statements are correct about a software switch on FortiGate? (Choose two.)

- A. It can be configured only when FortiGate is operating in NAT mode
- B. Can act as a Layer 2 switch as well as a Layer 3 router
- C. All interfaces in the software switch share the same IP address
- D. It can group only physical interfaces

**Answer:** AC

#### NEW QUESTION 2

Refer to the exhibit.

STUDENT # get system session list					
PROTO	EXPIRE	SOURCE	SOURCE-NAT	DESTINATION	DESTINATION-NAT
tcp	3598	10.0.1.10:2706	10.200.1.6:2706	10.200.1.254:80	-
tcp	3598	10.0.1.10:2704	10.200.1.6:2704	10.200.1.254:80	-
tcp	3596	10.0.1.10:2702	10.200.1.6:2702	10.200.1.254:80	-
tcp	3599	10.0.1.10:2700	10.200.1.6:2700	10.200.1.254:443	-
tcp	3599	10.0.1.10:2698	10.200.1.6:2698	10.200.1.254:80	-
tcp	3598	10.0.1.10:2696	10.200.1.6:2696	10.200.1.254:443	-
udp	174	10.0.1.10:2694	-	10.0.1.254:53	-
udp	173	10.0.1.10:2690	-	10.0.1.254:53	-

Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

- A. Destination NAT is disabled in the firewall policy.
- B. One-to-one NAT IP pool is used in the firewall policy.
- C. Overload NAT IP pool is used in the firewall policy.
- D. Port block allocation IP pool is used in the firewall policy.

**Answer:** B

#### Explanation:

FortiGate\_Security\_6.4 page 155 . In one-to-one, PAT is not required.

#### NEW QUESTION 3

Which two statements are correct about NGFW Policy-based mode? (Choose two.)

- A. NGFW policy-based mode does not require the use of central source NAT policy
- B. NGFW policy-based mode can only be applied globally and not on individual VDOMs
- C. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
- D. NGFW policy-based mode policies support only flow inspection

**Answer:** CD

#### NEW QUESTION 4

Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

- A. By default, FortiGate uses WINS servers to resolve names.
- B. By default, the SSL VPN portal requires the installation of a client's certificate.
- C. By default, split tunneling is enabled.
- D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

**Answer:** D

#### NEW QUESTION 5

Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

- A. DNS
- B. ping
- C. udp-echo
- D. TWAMP

**Answer:** CD

#### NEW QUESTION 6

Refer to the exhibit.

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.

New RADIUS Server

Name

FortiAuthenticator-RADIUS

Authentication method

Default

Specify

NAS IP

Include in every user group

☒

Primary Server

IP/Name

10.0.1.149

Secret

••••••••

Test Connectivity

Test User Credentials

What is the impact of using the Include in every user group option 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 all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
- D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

**Answer: A**

#### NEW QUESTION 7

Refer to the exhibits.

The exhibits show a network diagram and firewall configurations.

An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2. Remote-User1 must be able to access the Webserver. Remote-User2 must not be able to access the Webserver.

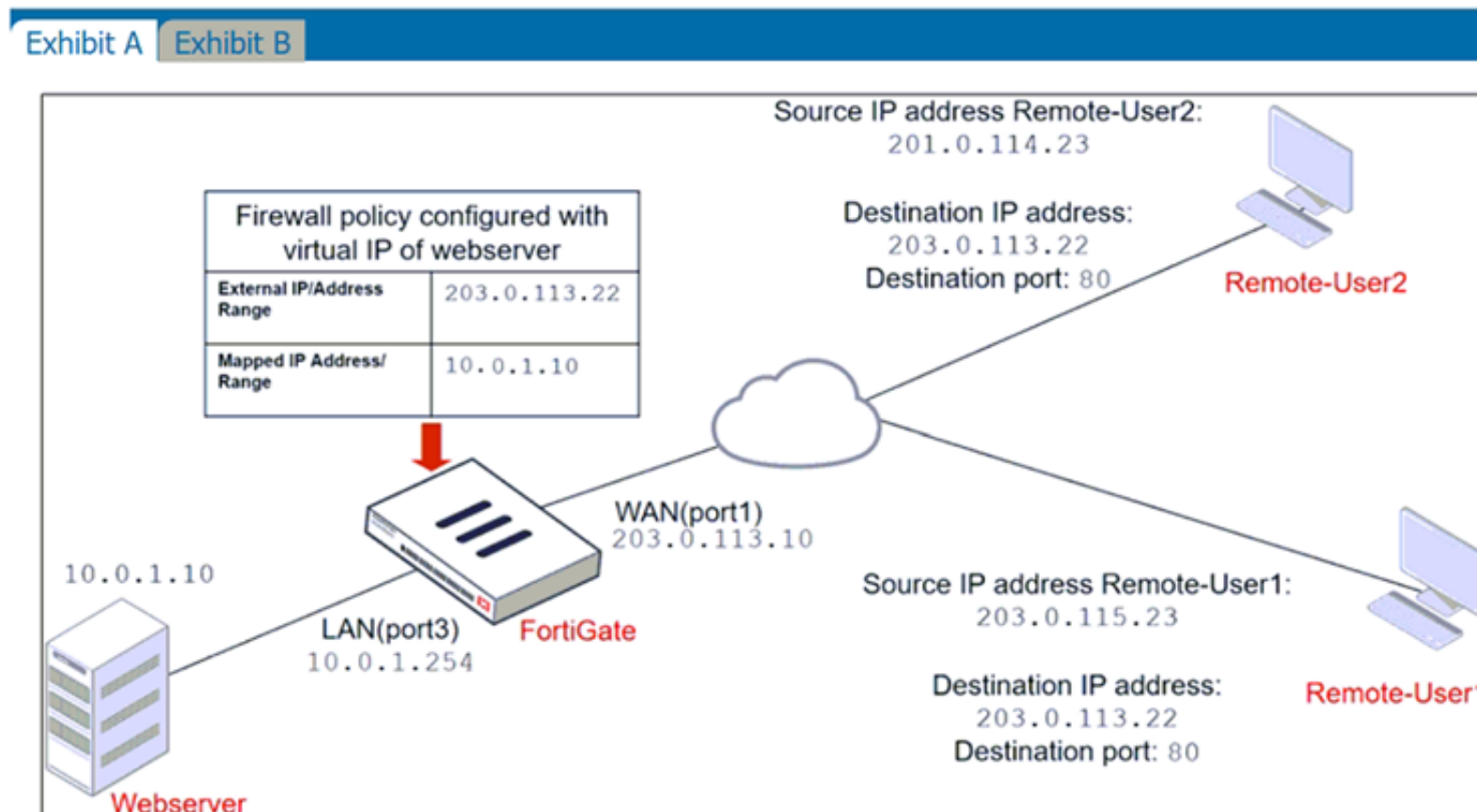


Exhibit A Exhibit B

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 address object

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

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

- A. Disable match-vip in the Deny policy.
- B. Set the Destination address as Deny\_IP in the Allow-access policy.
- C. Enable match vip in the Deny policy.
- D. Set the Destination address as Web\_server in the Deny policy.

**Answer: CD**

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta>

### NEW QUESTION 8

An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

- A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
- B. Create a new service object for HTTP service and set the session TTL to never
- C. Set the TTL value to never under config system-ttl
- D. Set the session TTL on the HTTP policy to maximum

**Answer: BC**

### NEW QUESTION 9

Refer to the exhibit.

HQ-FortiGate

IPsec

Remote-FortiGate

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name

ToRemote

Comments

Comments

Local Address

Subnet

0.0.0.0/0.0.0.0

Remote Address

Subnet

0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Add

Encryption

AES128

Authentication

SHA1

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group

32

31

30

29

28

27

21

20

19

18

17

16

15

14

5

2

1

Local Port

All

Remote Port

All

Protocol

All

Auto-negotiate

Autokey Keep Alive

Key Lifetime

Seconds

43200

Phase 2 Selectors

Name	Local Address	Remote Address
ToRemote	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

Edit Phase 2

Name

ToRemote

Comments

Comments

Local Address

Subnet

0.0.0.0/0.0.0.0

Remote Address

Subnet

0.0.0.0/0.0.0.0

Advanced...

Phase 2 Proposal

Add

Encryption

AES256

Authentication

SHA1

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group

32

31

30

29

28

27

21

20

19

18

17

16

15

14

5

2

1

Local Port

All

Remote Port

All

Protocol

All

Auto-negotiate

Autokey Keep Alive

Key Lifetime

Seconds

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, what configuration change will bring phase 2 up?

- A. On HQ-FortiGate, enable Auto-negotiate.
- B. On Remote-FortiGate, set Seconds to 43200.
- C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
- D. On HQ-FortiGate, set Encryption to AES256.

**Answer: D**

#### NEW QUESTION 10

Which two statements are true about the FGCP protocol? (Choose two.)

- A. FGCP elects the primary FortiGate device.
- B. FGCP is not used when FortiGate is in transparent mode.
- C. FGCP runs only over the heartbeat links.
- D. FGCP is used to discover FortiGate devices in different HA groups.

**Answer: AC**

#### Explanation:

The FGCP (FortiGate Clustering Protocol) is a protocol that is used to manage high availability (HA) clusters of FortiGate devices. It performs several functions, including the following:

FGCP elects the primary FortiGate device: In an HA cluster, FGCP is used to determine which FortiGate device will be the primary device, responsible for handling traffic and making decisions about what to allow or block. FGCP uses a variety of factors, such as the device's priority, to determine which device should be the primary.

FGCP runs only over the heartbeat links: FGCP communicates between FortiGate devices in the HA cluster using the heartbeat links. These are dedicated links that are used to exchange status and control information between the devices. FGCP does not run over other types of links, such as data links.

#### NEW QUESTION 10

FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.

In this scenario, which statement about VLAN IDs is true?

- A. The two VLAN subinterfaces can have the same VLAN ID only if they belong to different VDOMs.
- B. The two VLAN subinterfaces must have different VLAN IDs.
- C. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
- D. The two VLAN subinterfaces can have the same VLAN ID only if they have IP addresses in different subnets.

**Answer: CD**

#### NEW QUESTION 12

An administrator must disable RPF check to investigate an issue.

Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

- A. Enable asymmetric routing, so the RPF check will be bypassed.
- B. Disable the RPF check at the FortiGate interface level for the source check.
- C. Disable the RPF check at the FortiGate interface level for the reply check .
- D. Enable asymmetric routing at the interface level.

**Answer: B**

#### NEW QUESTION 14

Refer to the exhibit, which contains a session diagnostic output.

```
session info: proto=17 proto_state=01 duration=254 expire=179 timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ helper=dns-udp vlan_cos=0/255
state=log may_dirty f00 log-start
statistic(bytes/packets/allow_err): org=1420/22/1 reply=5678/22/1 tuples=2
tx speed(Bps/kbps): 5/0 rx speed(Bps/kbps): 22/0
origin->sink: org pre->post, reply pre->post dev=5->3/3->5 gwy=10.200.1.254/10.0.1.200
hook=post dir=org act=snat 10.0.1.200:2486->208.91.112.53:53(10.200.1.1:62902)
hook=pre dir=reply act=dnat 208.91.112.53:53->10.200.1.1:62902(10.0.1.200:2486)
misc=0 policy_id=3 auth_info=0 chk_client_info=0 vd=0
serial=0001fc1e tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which statement is true about the session diagnostic output?

- A. The session is a UDP unidirectional state.
- B. The session is in TCP ESTABLISHED state.
- C. The session is a bidirectional UDP connection.
- D. The session is a bidirectional TCP connection.

**Answer:** C

**Explanation:**

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

**NEW QUESTION 19**

Refer to the exhibit.

	Name	Type	IP/Netmask	VLAN ID
Physical Interface 14				
	port1	Physical Interface	10.200.1.1/255.255.255.0	
	port1-vlan10	VLAN	10.1.10.1/255.255.255.0	10
	port1-vlan1	VLAN	10.200.5.1/255.255.255.0	1
	port10	Physical Interface	10.0.11.1/255.255.255.0	
	port2	Physical Interface	10.200.2.1/255.255.255.0	
	port2-vlan10	VLAN	10.0.10.1/255.255.255.0	10
	port2-vlan1	VLAN	10.0.5.1/255.255.255.0	1

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

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

**Answer:** CD

**Explanation:**

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf>

<https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883>

**NEW QUESTION 20**

Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?

- A. The public key of the web server certificate must be installed on the browser.
- B. The web-server certificate must be installed on the browser.
- C. The CA certificate that signed the web-server certificate must be installed on the browser.
- D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

**Answer:** C

**NEW QUESTION 24**

Which statement about video filtering on FortiGate is true?

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

**Answer:** B

**NEW QUESTION 28**

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

**Answer:** D

**NEW QUESTION 29**

Refer to the exhibits.

**Edit Policy**

Name ⓘ Facebook SSL Inspection

Incoming interface  port2

Outgoing interface  port1

Source  all

Destination  all

Service  ALL

**Firewall/Network Options**


ⓘ CentralNAT is enabled so NAT settings from matching Central SNAT policies will be applied


**Security Profiles**


SSL Inspection  certificate-inspection


**Edit Policy**


Name ⓘ Facebook Access


Incoming interface  port2





Outgoing interface  port1




Source  all

Destination  all


Schedule  always

Service  AppDefault Specify

Application Facebook   
 Facebook\_Like.Button    
 Facebook\_Video.Play 

URL Category   
 ACCEPT  DENY

**Firewall/Network Options**

Protocol Options  default

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) for Facebook .

Users are given access to the Facebook web application. They can play video content hosted on Facebook but they are unable to leave reactions on videos or other types of posts.

Which part of the policy configuration must you change to resolve the issue?

- A. Make SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Get the additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

**Answer:** A

**Explanation:**

They can play video (tick) content hosted on Facebook, but they are unable to leave reactions on videos or other types of posts. This indicate that the rule are partially working as they can watch video but cant react, i.e. liking the content. So must be an issue with the SSL inspection rather then adding an app rule.

**NEW QUESTION 30**

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

- A. It provides executive summaries of the four largest areas of security focus.
- B. Many of the security issues can be fixed immediately by clicking Apply where available.
- C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
- D. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.

**Answer:** BC

**NEW QUESTION 34**

Refer to the exhibits.  
 Exhibit A.



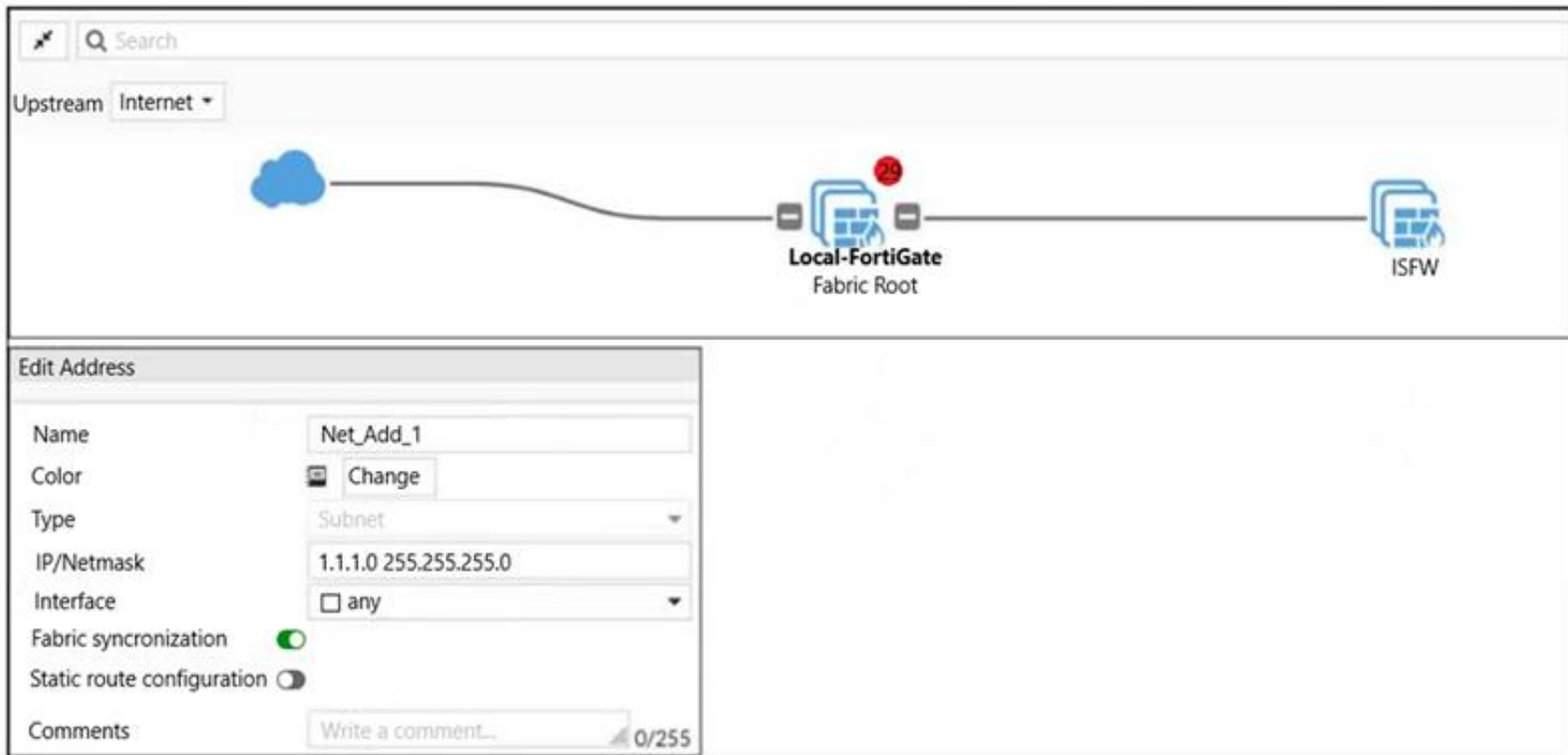


Exhibit B.

```
Local-FortiGate # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 0.0.0.0
    set upstream-port 8013
    set group-name "fortinet"
    set group-password ENC X18CtzrcUBUq9yz9nryP+YfM16
    BJkv7S/trtoh2gYAe5CH8YMAa0GT18aX+/dKH/o5izw1ZEoN1QN2N
    FGLT4r5z2AyYI8i1PxutiLcsCp1AdZadv1CxDe66IdLX7I6o22J9P
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set fabric-object-unification local
    set saml-configuration-sync default
```

```
ISFW # show full-configuration system csf
config system csf
    set status enable
    set upstream-ip 10.0.1.254
    set upstream-port 8013
    set group-name ''
    set accept-auth-by-cert enable
    set log-unification enable
    set authorization-request-type serial
    set fabric-workers 2
    set downstream-access disable
    set configuration-sync default
    set saml-configuration-sync default
end

ISFW #
ISFW #
```

An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric. After synchronization, this object is not available on the downstream FortiGate (ISFW).

What must the administrator do to synchronize the address object?

- A. Change the csf setting on Local-FortiGate (root) to set configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to set configuration-sync local.
- C. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.
- D. Change the csf setting on ISFW (downstream) to set fabric-object-unification default.

**Answer: C**

#### NEW QUESTION 36

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

- A. To detect intermediary NAT devices in the tunnel path.
- B. To dynamically change phase 1 negotiation mode aggressive mode.
- C. To encapsulation ESP packets in UDP packets using port 4500.
- D. To force a new DH exchange with each phase 2 rekey.

**Answer: AC**

#### NEW QUESTION 39

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

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

**Answer: CD**

#### Explanation:

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

#### NEW QUESTION 40

Examine this PAC file configuration.

Which of the following statements are true? (Choose two.)



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

**Answer:** AD

#### NEW QUESTION 41

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

- A. Policy lookup will be disabled.
- B. By Sequence view will be disabled.
- C. Search option will be disabled
- D. Interface Pair view will be disabled.

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 45

A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. 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 the file can be downloaded. What is the reason for the failed virus detection by FortiGate?

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

**Answer:** AD

#### Explanation:

https traffic requires SSL decryption. Check the ssh inspection profile

#### NEW QUESTION 46

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

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

**Answer:** AC

#### NEW QUESTION 48

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

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

**Answer:** BDE

#### NEW QUESTION 50

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

**Answer:** AB

#### NEW QUESTION 55

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

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

**Answer:** D

NEW QUESTION 59

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

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

Answer: AD

Explanation:

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

NEW QUESTION 64

Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

- A. diagnose wad session list
- B. diagnose wad session list | grep hook-pre&&hook-out
- C. diagnose wad session list | grep hook=pre&&hook=out
- D. diagnose wad session list | grep "hook=pre"&"hook=out"

Answer: A

NEW QUESTION 68

Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

- A. The firmware image must be manually uploaded to each FortiGate.
- B. Only secondary FortiGate devices are rebooted.
- C. Uninterruptable upgrade is enabled by default.
- D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 73

Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

- A. FortiGuard web filter cache
- B. FortiGate hostname
- C. NTP
- D. DNS

Answer: CD

NEW QUESTION 75

Refer to exhibit.

An administrator configured the web filtering profile shown in the exhibit to block access to all social networking sites except Twitter. However, when users try to access twitter.com, they are redirected to a FortiGuard web filtering block page.

Name: Allow\_Twitter

Comments: Write a comment... 0/255

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

☒ FortiGuard Category Based Filter

☒ Allow
 ☐ Monitor
 ☐ Block
 ☐ Warning
 ☐ Authenticate

Name	Action
Medicine	<input checked="" type="checkbox"/> Allow
News and Media	<input checked="" type="checkbox"/> Allow
Social Networking	<input type="checkbox"/> Block
Political Organizations	<input checked="" type="checkbox"/> Allow
Reference	<input checked="" type="checkbox"/> Allow
Global Religion	<input checked="" type="checkbox"/> Allow
Shopping	<input checked="" type="checkbox"/> Allow
Society and Lifestyles	<input checked="" type="checkbox"/> Allow
Sports	<input checked="" type="checkbox"/> Allow

**Static URL Filter**

Block invalid URLs: ☐

URL Filter: ☒

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

URL	Type	Action	Status
twitter.com	Wildcard	<input checked="" type="checkbox"/> Allow	<input checked="" type="checkbox"/> Enable

Block malicious URLs discovered by FortiSandbox: ☐

Content Filter: ☐

Based on the exhibit, which configuration change can the administrator make to allow Twitter while blocking all other social networking sites?

- A. On the FortiGuard Category Based Filter configuration, set Action to Warning for Social Networking
- B. On the Static URL Filter configuration, set Type to Simple
- C. On the Static URL Filter configuration, set Action to Exempt.

D. On the Static URL Filter configuration, set Action to Monitor.

**Answer:** C

#### NEW QUESTION 79

Which two statements are true about the RPF check? (Choose two.)

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

**Answer:** AD

#### NEW QUESTION 80

Refer to the exhibit.



```
session info: proto=6 proto_state=02 duration=6 expire=6 timeout=3600 flags=0000
0000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty
statistic(bytes/packets/allow_err): org=180/3/1 reply=264/3/1 tuples=2
tx speed(Bps/kbps): 26/0 rx speed(Bps/kbps): 39/0
origin->sink: org pre->post, reply pre->post dev=3->5/5->3 gwy=10.0.1.11/0.0.0.0
hook=pre dir=org act=dnat 10.200.3.1:38024->10.200.1.11:80(10.0.1.11:80)
hook=post dir=reply act=snat 10.0.1.11:80->10.200.3.1:38024(10.200.1.11:80)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=8 auth_info=0 chk_client_info=0 vd=0
serial=0001fb06 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id= 00000000 rpdb_svc_id=0 ngfwid=n/a
npu_state=0x040000
```

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

- A. The session is in SYN\_SENT state.
- B. The session is in FIN\_ACK state.
- C. The session is in FTN\_WAIT state.
- D. The session is in ESTABLISHED state.

**Answer:** A

#### Explanation:

Indicates TCP (proto=6) session in SYN\_SENT state (proto=state=2) <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

#### NEW QUESTION 81

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

**Answer:** AC

#### NEW QUESTION 83

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 no traffic is observed in the tunnel.

Which DPD mode on FortiGate will meet the above requirement?

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

**Answer:** D

#### NEW QUESTION 88

Which two statements about FortiGate FSSO agentless polling mode are true? (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

**Explanation:**

You can deploy FSSO w/o installing an agent. FG polls the DCs directly, instead of receiving logon info indirectly from a collector agent. Because FG collects all of the data itself, agentless polling mode requires greater system resources, and it doesn't scale as easily. Agentless polling mode operates in a similar way to WinSecLog, but with only two event IDs: 4768 and 4769. Because there's no collector agent, FG uses the SMB protocol to read the event viewer logs from the DCs. FG acts as a collector. It 's responsible for polling on top of its normal FSSO tasks but does not have all the extra features, such as workstation checks, that are available with the external collector agent.

**NEW QUESTION 92**

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

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

**Answer:** B

**NEW QUESTION 94**

Which statement is correct regarding the use of application control for inspecting web applications?

- A. Application control can identity child and parent applications, and perform different actions on them.
- B. Application control signatures are organized in a nonhierarchical structure.
- C. Application control does not require SSL inspection to identity web applications.
- D. Application control does not display a replacement message for a blocked web application.

**Answer:** A

**Explanation:**

Application control is a feature that allows FortiGate to inspect and control the use of specific web applications on the network. When application control is enabled, FortiGate can identify child and parent applications, and can perform different actions on them based on the configuration.

**NEW QUESTION 96**

Refer to the exhibits.



SSL-VPN Settings

Connection Settings ⓘ

Listen on Interface(s)

port1

+

×

Listen on Port

10443

Web mode access will be listening at

https://10.200.1.1:10443

Redirect HTTP to SSL-VPN

☐

Restrict Access

Allow access from any host

Limit access to specific hosts

Idle Logout

☒

Inactive For

300

Seconds

Server Certificate

Fortinet\_Factory

▼

Require Client Certificate

☐

Tunnel Mode Client Settings ⓘ

Address Range

Automatically assign addresses

Specify custom IP ranges

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

DNS Server

Same as client system DNS

Specify

Specify WINS Servers

☐

Authentication/Portal Mapping ⓘ

+ Create New

✎ Edit

🗑 Delete

Users/Groups ⌵	Portal ⌵
👤 sslvpn	tunnel-access
All Other Users/Groups	full-access

Connection status

Connection:

VPN

Server:

https://10.200.1.1:1443/

Status:

Connecting...

Duration:

—

Bytes received:

0

Bytes sent:

0

Stop

The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?

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

Answer: A

NEW QUESTION 101

Which three statements are true regarding session-based authentication? (Choose three.)

- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.

- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

**Answer:** ACD

#### NEW QUESTION 104

Which statement about the policy ID number of a firewall policy is true?

- A. It is required to modify a firewall policy using the CLI.
- B. It represents the number of objects used in the firewall policy.
- C. It changes when firewall policies are reordered.
- D. It defines the order in which rules are processed.

**Answer:** A

#### NEW QUESTION 105

Which three security features require the intrusion prevention system (IPS) engine to function? (Choose three.)

- A. Web filter in flow-based inspection
- B. Antivirus in flow-based inspection
- C. DNS filter
- D. Web application firewall
- E. Application control

**Answer:** ABE

#### Explanation:

<https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow>

#### NEW QUESTION 109

Which two statements are true when FortiGate is in transparent mode? (Choose two.)

- A. By default, all interfaces are part of the same broadcast domain.
- B. The existing network IP schema must be changed when installing a transparent mode.
- C. Static routes are required to allow traffic to the next hop.
- D. FortiGate forwards frames without changing the MAC address.

**Answer:** AD

#### NEW QUESTION 110

Refer to the exhibit.



The screenshot shows the FortiGate SLA configuration page. The 'Name' field is 'SLA1'. Under 'Protocol', 'Ping' is selected. The 'Server' field contains two entries: '4.2.2.2' and '4.2.2.1'. Under 'Participants', 'All SD-WAN Members' is selected. Below that, 'port1' and 'port2' are listed. At the bottom, the 'Enable probe packets' toggle is turned off.

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

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

**Answer:** BD

#### NEW QUESTION 112

Refer to the FortiGuard connection debug output.

```
FortiGate # diagnose debug rating
Locale      : english

Service     : Web-Filter
Status      : Enable
License     : Contract

Num. of servers : 3
Protocol     : https
Port        : 443
Anycast     : Disable
Default servers : Included
-- Server List (Mon Jul 5 12:00:25 2021) --

IP           Weight  RTT  Flags  TZ  FortiGuard-requests  Curr  Lost  Total  Lost  Updated Time
173.243.138.210  10    350  DI    -8    29      0    0      0      0    Mon Jul 5 09:23:33 2021
12.34.97.18     20    30   -5    -5    25      0    0      0      0    Mon Jul 5 09:23:33 2021
210.7.96.18     160   605   9     9    25      0    0      0      0    Mon Jul 5 09:23:33 2021
```

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

- A. A local FortiManager is one of the servers FortiGate communicates with.
- B. One server was contacted to retrieve the contract information.
- C. There is at least one server that lost packets consecutively.
- D. FortiGate is using default FortiGuard communication settings.

**Answer:** BD

#### NEW QUESTION 116

Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites? A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.

- A. The application signature database inspects traffic only from the original web application server.
- B. FortiGuard maintains only one signature of each web application that is unique.
- C. FortiGate can inspect sub-application traffic regardless where it was originate

**Answer:** D

#### NEW QUESTION 119

.....

## 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 Practice Exam Features:

- \* NSE4 Questions and Answers Updated Frequently
- \* NSE4 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* NSE4 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE4 Practice Test Here](#)**