

# Fortinet

## Exam Questions NSE4\_FGT-6.4

Fortinet NSE 4 - FortiOS 6.4



NEW QUESTION 1

Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Exhibit A

Edit Policy

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

☒

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

☐

Protocol Options

PRX default

Security Profiles

AntiVirus

☒

AV default

Web Filter

☐

DNS Filter

☐

Application Control

☐

IPS

☐

SSL Inspection

☒

SSL deep-inspection

Decrypted Traffic Mirror

☐

Exhibit B

Edit AntiVirus Profile

Name

default

Comments

Scan files and block viruses.

29/255

Detect Viruses

Block

Monitor

Feature set

Flow-based

Proxy-based

Inspected Protocols

HTTP

☒

SMTP

☒

POP3

☒

IMAP

☒

FTP

☒

CIFS

☐

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses

☒

Include Mobile Malware Protection

☒

Virus Outbreak Prevention

☒

Use FortiGuard Outbreak Prevention Database

☐

Use External Malware Block List

☐

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

- A. The firewall policy performs the full content inspection on the file.
- B. The flow-based inspection is used, which resets the last packet to the user.

- C. The volume of traffic being inspected is too high for this model of FortiGate.  
D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

**Answer:** A

#### NEW QUESTION 2

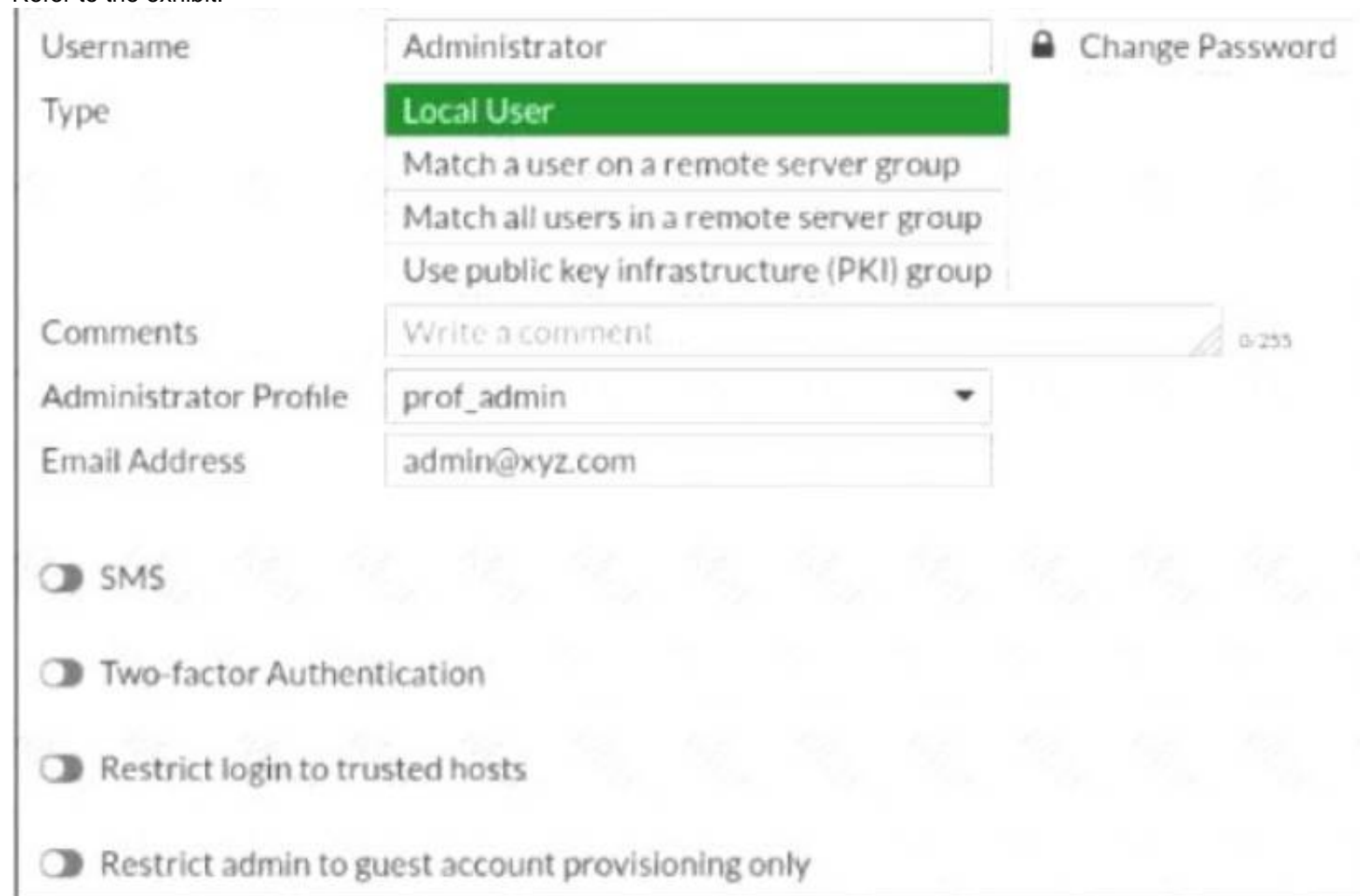
Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)

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

**Answer:** AB

#### NEW QUESTION 3

Refer to the exhibit.



The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?

- A. Change password  
B. Enable restrict access to trusted hosts  
C. Change Administrator profile  
D. Enable two-factor authentication

**Answer:** D

#### NEW QUESTION 4

Which two statements are 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 all FortiGate devices.

**Answer:** AC

#### NEW QUESTION 5

View the exhibit.

Application Details

| Name            | Category | Technology    | Popularity | Risk |
|-----------------|----------|---------------|------------|------|
| Addicting Games | Game     | Browser-Based | ☆☆☆☆       | Risk |

Application Control Profile

Categories

All Categories

Business (149, 6)

Email (80, 13)

Industrial (1168)

P2P (70)

SocialMedia (120, 31)

Video/Audio (164, 14)

Unknown Applications

Cloud.IT (42)

Game (83)

Mobile (3)

Proxy (148)

Storage.Backup (175, 17)

VoIP (27)

Collaboration (274, 10)

GeneralInterest (233, 6)

Network.Service (325)

Remote.Access (84)

Update (49)

Web.Client (22)

Application Overrides

+ Add Signatures

Edit Parameters

Delete

| Application Signature | Category | Action |
|-----------------------|----------|--------|
| Addicting Games       | Game     | Allow  |

Filter Overrides

+ Add Filter

Edit

Delete

| Filter Details  | Action |
|-----------------|--------|
| Risk (2304, 52) | Block  |

A user behind the FortiGate is trying to go to <http://www.addictinggames.com> (Addicting Games). Based on this configuration, which statement is true?

- A. Addicting.Games is allowed based on the Application Overrides configuration.
- B. Addicting.Games is blocked on the Filter Overrides configuration.
- C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
- D. Addicting.Games is allowed based on the Categories configuration.

**Answer: A**

#### NEW QUESTION 6

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

**Answer: C**

#### NEW QUESTION 7

View the exhibit.

Destination

Subnet

Named Address

Internet Service

172.13.24.0/255.255.255.0

Interface

TunnelB

Administrative Distance

5

Comments

0/255

Status

Enabled

Disabled

Advanced Options

Priority

30

Destination

Subnet

Named Address

Internet Service

172.13.24.0/255.255.255.0

Interface

TunnelA

Administrative Distance

10

Comments

0/255

Status

Enabled

Disabled

Advanced Options

Priority

0

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

- A. This setup requires at least two firewall policies with the action set to IPsec.
- B. Dead peer detection must be disabled to support this type of IPsec setup.
- C. The TunnelB route is the primary route for reaching the remote sit
- D. The TunnelA route is used only if the TunnelB VPN is down.
- E. This is a redundant IPsec setup.

**Answer: CD**

#### NEW QUESTION 8

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager



- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

**Answer:** B

#### NEW QUESTION 9

An administrator is configuring an IPsec VPN between site A and site B. The Remote Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.160.1.0/24 and the remote quick mode selector is 192.168.2.0/24. Which subnet must the administrator configure for the local quick mode selector for site B?

- A. 192.168.1.0/24
- B. 192.168.0.0/24
- C. 192.168.2.0/24
- D. 192.168.3.0/24

**Answer:** B

#### NEW QUESTION 10

Which three statements about a flow-based antivirus profile are correct? (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:** CDE

#### NEW QUESTION 10

Refer to the exhibit.

|                              | Name         | Type               | IP/Netmask               | VLAN ID |
|------------------------------|--------------|--------------------|--------------------------|---------|
| <b>Physical Interface</b> 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. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs
- B. port1 is a native VLAN.
- C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
- D. Traffic between port2 and port2-vlan1 is allowed by default.

**Answer:** CD

#### NEW QUESTION 11

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:** BD

#### NEW QUESTION 15

An administrator has configured a strict RPF check on FortiGate. Which statement is true about the strict RPF check?

- A. The strict RPF check is run on the first sent and reply packet of any new session.
- B. Strict RPF checks the best route back to the source using the incoming interface.
- C. Strict RPF checks only for the existence of at least one active route back to the source using the incoming interface.
- D. Strict RPF allows packets back to sources with all active routes.

Answer: A

**NEW QUESTION 18**

Refer to the exhibit.

**Outgoing Interfaces**

☐ Manual  
Manually assign outgoing interfaces.

☒ **Best Quality**  
The interface with the best measured performance is selected.

☐ **Lowest Cost (SLA)**  
The interface that meets SLA targets is selected. When there is a tie, the interface with the lowest assigned cost is selected.

☐ **Maximize Bandwidth (SLA)**  
Traffic is load balanced among interfaces that meet SLA targets.

**Interface preference**

- port1
- port2
- port3
- port4

**Measured SLA**: SLA\_1

**Quality criteria**: Latency

**Status**: ☒ Enable ☐ Disable

```
NGFW-1 # diagnose sys virtual-wan-link health-check
Health Check(DC_PBX_SLA):
Seq(1 port1): state(alive), packet-loss(0.000%) latency(21.566), jitter(2.685) sla_map=0x
Seq(2 port2): state(alive), packet-loss(0.000%) latency(54.349), jitter(4.287) sla_map=0x
Seq(3 port3): state(alive), packet-loss(0.100%) latency(32.683), jitter(5.685) sla_map=0x
Seq(4 port4): state(alive), packet-loss(2.010%) latency(48.881), jitter(4.287) sla_map=0x
```

The exhibit contains the configuration for an SD-WAN Performance SLA, as well as the output of diagnose sys virtual-wan-link health-check. Which interface will be selected as an outgoing interface?

- A. port2
- B. port4
- C. port3
- D. port1

Answer: B

**NEW QUESTION 23**

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.
- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

Answer: CD

**NEW QUESTION 26**

Refer to the exhibit showing a debug flow output.

```
id=20085 trace_id=1 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1, 10.0.1.10:19938->10.0.1.250:2048) from port1. type=8, code=0, id=19938, seq=1."
id=20085 trace_id=1 func=init_ip_session_common line=5760 msg="allocate a new session-00003dd5"
id=20085 trace_id=1 func=vf_ip_route_input_common line=2598 msg="find a route: flag=84000000 gw=10.0.1.250 via root"
id=20085 trace_id=2 func=print_pkt_detail line=5594 msg="vd-root:0 received a packet(proto=1, 10.0.1.250:19938->10.0.1.10:0) from local. type=0, code=0, id=19938, seq=1."
id=20085 trace_id=2 func=resolve_ip_tuple_fast line=5675 msg="Find an existing session, id=00003dd5, reply direction"
```

Which two statements about the debug flow output are correct? (Choose two.)

- A. The debug flow is of ICMP traffic.
- B. A firewall policy allowed the connection.

- C. A new traffic session is created.
- D. The default route is required to receive a reply.

**Answer:** B

#### NEW QUESTION 29

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check.

**Answer:** D

#### NEW QUESTION 33

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 35

An administrator is running the following sniffer command:

```
diagnose sniffer packet any "host 192.168.2.2" 5
```

Which three pieces of information will be included in the sniffer output? (Choose three.)

- A. Interface name
- B. Packet payload
- C. Ethernet header
- D. IP header
- E. Application header

**Answer:** BCE

#### NEW QUESTION 38

A network administrator is configuring a new IPsec VPN tunnel on FortiGate. The remote peer IP address is dynamic, in addition, the remote peer does not support a dynamic DNS update service. What type of remote gateway should the administrator configure on FortiGate for the new IPsec VPN tunnel to work?

- A. Static IP Address
- B. Dialup User
- C. Dynamic DNS
- D. Pre-shared Key

**Answer:** C

#### NEW QUESTION 41

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\_SEXT 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: D

NEW QUESTION 43

An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

- A. A phase 2 configuration is not required.
- B. This VPN cannot be used as part of a hub-and-spoke topology.
- C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
- D. The IPsec firewall policies must be placed at the top of the list.

Answer: C

Explanation:

In a route-based configuration, FortiGate automatically adds a virtual interface eith the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION 44

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.

IPS Sensor

Edit IPS Sensor

WINDOWS\_SERVER

Name

EMAIL-SERVER-IPS

[View IPS Signatures]

Comments

view

IPS Signatures

+ Add Signatures

Delete

Edit IP Exemptions

| Name                | Exempt IPs | Severity | Target | Service  | OS  | Action | Packet Logging |
|---------------------|------------|----------|--------|----------|-----|--------|----------------|
| SMTPLoginBruteForce |            | High     | Server | TCP SMTP | All | Block  |                |

IPS Filters

+ Add Filter

Edit Filter

Delete

| Filter Details                     | Action | Packet Logging |
|------------------------------------|--------|----------------|
| Location: server<br>Protocol: SMTP | Block  |                |

Rate Based Signatures

| Enable                              | Signature   | Threshold | Duration(seconds) | Track By  | Action | Block Duration(minutes) |
|-------------------------------------|---|-----------|-------------------|-----------|--------|-------------------------|
| <input checked="" type="checkbox"/> | IMAPLoginBruteForce<br><small>Primary Exhaustion (2x)</small> | 60        | 10                | Source IP | Block  | None                    |
| <input checked="" type="checkbox"/> | Outgoing SMTP TLS TCP Connection Close (2x)                   | 1         | 1                 | Any       | Block  | None                    |

Apply

DoS Policy

Incoming Interface

port1

Source Address

all

+

×

Destination Address

all

+

×

Services

ALL

+

×

L3 Anomalies

| Name           | Status                   | Logging                  | Pass | Block | Action |
|----------------|--------------------------|--------------------------|------|-------|--------|
| ip_src_session | <input type="checkbox"/> | <input type="checkbox"/> | Pass | Block |        |
| ip_dst_session | <input type="checkbox"/> | <input type="checkbox"/> | Pass | Block |        |

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip\_src\_session
- D. Location: server Protocol: SMTP

Answer: B

NEW QUESTION 48

Examine the following web filtering log.



```
Date=2016-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk level=warning
vd=root policyid=1 sessionid=149645 user= " " scrip=10.0.1.10 srcport=52919 srcintf= "port3"
dstip=54.230.128.169 dstport=80 dstintf= "port1" proto=6 service="HTTP" hostname= "miniclip.com"
profile= "default" action=blocked regtype=direct url= "/" sentbyte=286 rcvdbyte=0 direction=outgoing msg= "URL
belongs to a category with warnings enabled" method=domain cat=20 catdesc="Games" crscore=30 crlevel=high
```

Which statement about the log message is true?

- A. The action for the category Games is set to block.
- B. The usage quota for the IP address 10.0.1.10 has expired
- C. The name of the applied web filter profile is default.
- D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

**Answer: C**

#### NEW QUESTION 53

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

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

**Answer: A**

#### NEW QUESTION 57

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.

- \*All traffic must be routed through the primary tunnel when both tunnels are up
- \*The secondary tunnel must be used only if the primary tunnel goes down
- \*In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover

Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

- A. Enable Dead Peer Detection.
- B. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- C. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
- D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

**Answer: A**

#### NEW QUESTION 62

Refer to the exhibit.

| Field                   | Value  |
|-------------------------|--|
| Version                 | V3   |
| Serial Number           | 98765432   |
| Signature algorithm     | SHA256RSA  |
| Issuer                  | cn=RootCA,o=BridgeAuthority, Inc., c=US  |
| Valid from              | Tuesday, October 3, 2016 4:33:37 PM  |
| Valid to                | Wednesday, October 2, 2019 5:03:37 PM  |
| Subject                 | cn=John Doe, o=ABC, Inc., c=US   |
| Public key              | RSA (2048 bits)  |
| Key Usage               | keyCertSign  |
| Extended Key Usage      | Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2) |
| Basic Constraints       | CA=True, Path Constraint=None  |
| CRL Distribution Points | URL=http://webserver.abcinc.com/arlcert.crl  |

According to the certificate values shown in the exhibit, which type of entity was the certificate issued to?

- A. A user
- B. A root CA
- C. A bridge CA
- D. A subordinate

**Answer: A**

#### NEW QUESTION 63

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 65

Refer to the exhibits.

**Exhibit A**

Edit Policy

|                    |                         |  |
|--------------------|-------------------------|--|
| Name               | Facebook SSL Inspection |  |
| Incoming Interface | port2                   |  |
| Outgoing Interface | port1                   |  |
| Source             | all                     |  |
| Destination        | all                     |  |
| Service            | ALL                     |  |

Firewall / Network Options

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

Security Profiles

SSL Inspection certificate-inspection

**Exhibit B**

Edit Policy

|                            |                      |         |
|----------------------------|----------------------|---------|
| Name                       | Facebook Access      |         |
| Incoming Interface         | port2                |         |
| Outgoing Interface         | port1                |         |
| Source                     | all                  |         |
| Destination                | all                  |         |
| Schedule                   | always               |         |
| Service                    | App Default          | Specify |
| Application                | Facebook             |         |
|                            | Facebook_Like.Button |         |
|                            | Facebook_Video.Play  |         |
| URL Category               |                      |         |
| Action                     | 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. The SSL inspection needs to be a deep content inspection.
- B. Force access to Facebook using the HTTP service.
- C. Additional application signatures are required to add to the security policy.
- D. Add Facebook in the URL category in the security policy.

**Answer:** A

**NEW QUESTION 67**

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

- A. remote user's public IP address
- B. The public IP address of the FortiGate device.
- C. The remote user's virtual IP address.
- D. The internal IP address of the FortiGate device.

**Answer:** D

**Explanation:**

Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

**NEW QUESTION 71**

Which statement regarding the firewall policy authentication timeout is true?

- A. It is an idle timeout
- B. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
- C. It is a hard timeout
- D. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
- E. It is an idle timeout
- F. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
- G. It is a hard timeout
- H. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.

**Answer: A**

#### NEW QUESTION 75

Refer to the exhibit.

The diagram illustrates an IPsec tunnel between two FortiGate devices: HQ-FortiGate and Remote-FortiGate. Below the diagram, two screenshots of the FortiGate configuration interface are shown, detailing the Phase 2 selectors for the tunnel.

**HQ-FortiGate Configuration:**

- 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
  - Local Address: Subnet 0.0.0.0/0.0.0.0
  - Remote Address: Subnet 0.0.0.0/0.0.0.0
  - Phase 2 Proposal: Add
  - Encryption: AES128
  - Authentication: SHA1
  - Enable Replay Detection: ☒
  - Enable Perfect Forward Secrecy (PFS): ☒
  - Diffie-Hellman Group: 5
  - Local Port: All ☒
  - Remote Port: All ☒
  - Protocol: All ☒
  - Auto-negotiate: ☐
  - Autokey Keep Alive: ☐
  - Key Lifetime: Seconds 43200

**Remote-FortiGate Configuration:**

- Phase 2 Selectors:**

| Name | Local Address   | Remote Address  |
|------|-----------------|-----------------|
| ToHQ | 0.0.0.0/0.0.0.0 | 0.0.0.0/0.0.0.0 |
- Edit Phase 2:**
  - Name: ToHQ
  - Local Address: Subnet 0.0.0.0/0.0.0.0
  - Remote Address: Subnet 0.0.0.0/0.0.0.0
  - Phase 2 Proposal: Add
  - Encryption: AES256
  - Authentication: SHA1
  - Enable Replay Detection: ☒
  - Enable Perfect Forward Secrecy (PFS): ☒
  - Diffie-Hellman Group: 5
  - 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?

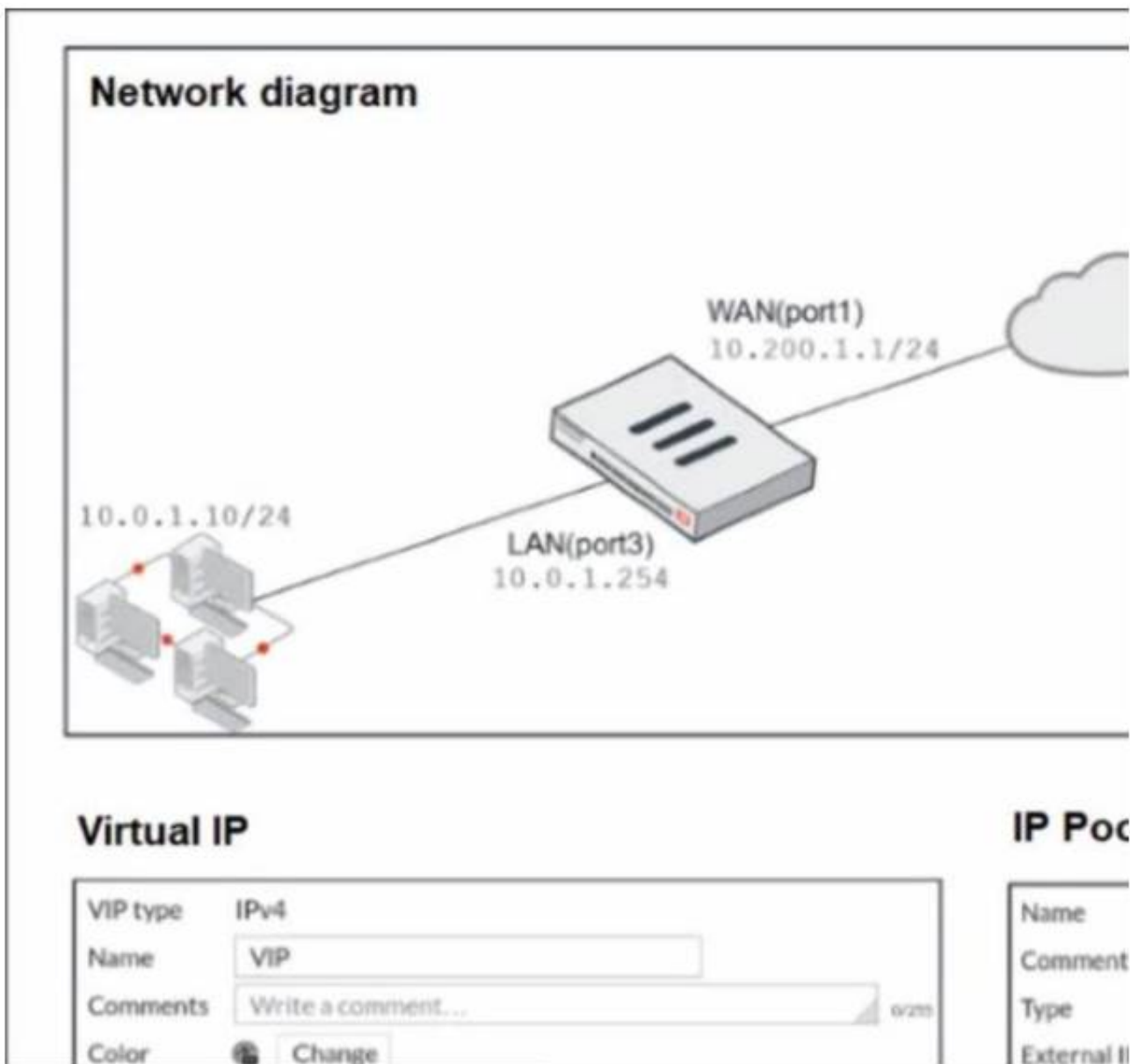
- A. On HQ-FortiGate, enable Auto-negotiate.
- B. On Remote-FortiGate, set Seconds to 43200.
- C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
- D. On HQ-FortiGate, set Encryption to AES256.

**Answer: D**

#### NEW QUESTION 79

Refer to the exhibit.





The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration. The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port3) interface has the IP address 10.0.1.254/24. The first firewall policy has NAT enabled using IP Pool. The second firewall policy is configured with a VIP as the destination address. Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0.1.10?

- A. 10.200.1.1
- B. 10.200.3.1
- C. 10.200.1.100
- D. 10.200.1.10

**Answer:** A

#### NEW QUESTION 81

Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

- A. To remove the NAT operation.
- B. To generate logs
- C. To finish any inspection operations.
- D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

**Answer:** D

#### NEW QUESTION 85

Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {
  if (shExpMatch (url, "*.fortinet.com/*")) {
    return "DIRECT";
  }
  if (isInNet (host, "172.25.120.0", "255.255.255.0")) {
    return "PROXY altproxy.corp.com: 8060";
  }
  return "PROXY proxy.corp.com: 8090";
}
```

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 90



Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

- A. This is known as many-to-one NAT.
- B. Source IP is translated to the outgoing interface IP.
- C. Connections are tracked using source port and source MAC address.
- D. Port address translation is not used.

**Answer:** AB

#### NEW QUESTION 92

Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

- A. System time
- B. FortiGuard update servers
- C. Operating mode
- D. NGFW mode

**Answer:** AD

#### NEW QUESTION 96

Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

- A. hard-timeout
- B. auth-on-demand
- C. soft-timeout
- D. new-session
- E. Idle-timeout

**Answer:** ADE

#### Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221>

#### NEW QUESTION 98

An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

- A. Add the support of NTLM authentication.
- B. Add useraccounts to Active Directory (AD).
- C. Add user accounts to the FortiGate group filter.
- D. Add user accounts to the Ignore User List.

**Answer:** C

#### NEW QUESTION 102

Examine this FortiGate configuration:

```
config authentication setting
    set active-auth-scheme SCHEME1
end
config authentication rule
    edit WebProxyRule
        set srcaddr 10.0.1.0/24
        set active-auth-method SCHEME2
    next
end
```

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

- A. It always authorizes the traffic without requiring authentication.
- B. It drops the traffic.
- C. It authenticates the traffic using the authentication scheme SCHEME2.
- D. It authenticates the traffic using the authentication scheme SCHEME1.

**Answer:** D

#### Explanation:

“What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting”

#### NEW QUESTION 105

Refer to the exhibit.



Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. The signature setting uses a custom rating threshold.
- B. The signature setting includes a group of other signatures.
- C. Traffic matching the signature will be allowed and logged.
- D. Traffic matching the signature will be silently dropped and logged.

Answer: B

NEW QUESTION 110

Examine the two static routes shown in the exhibit, then answer the following question.

| + Create New   Edit   Clone   Delete |              |           |          |          |
|--------------------------------------|--------------|-----------|----------|----------|
| Destination                          | Gateway      | Interface | Priority | Distance |
| 172.20.168.0/24                      | 172.25.176.1 | port1     | 10       | 20       |
| 172.20.168.0/24                      | 172.25.178.1 | port2     | 20       | 20       |

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

- A. FortiGate will load balance all traffic across both routes.
- B. FortiGate will use the port1 route as the primary candidate.
- C. FortiGate will route twice as much traffic to the port2 route
- D. FortiGate will only actuate the port1 route in the routing table

Answer: B

Explanation:

“If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path.”

NEW QUESTION 111

An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

Answer: ABC

Explanation:

[https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top\\_VirtualWirePair.htm](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm)

NEW QUESTION 115

.....

## 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-6.4 Practice Exam Features:

- \* NSE4\_FGT-6.4 Questions and Answers Updated Frequently
- \* NSE4\_FGT-6.4 Practice Questions Verified by Expert Senior Certified Staff
- \* NSE4\_FGT-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* NSE4\_FGT-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The NSE4\\_FGT-6.4 Practice Test Here](#)**