

## NSE4\_FGT-6.2

Number: NSE4\_FGT-6.2

Passing Score: 800

Time Limit: 120 min

File Version: 1

NSE4\_FGT-6.2



**Website:** <https://vceplus.com>

**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>

**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>

**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

<https://vceplus.com/>

## Exam A

### QUESTION 1

In an HA cluster operating in active-active mode, which path is taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?



<https://vceplus.com/>

- A. Client > secondary FortiGate > primary FortiGate > web server
- B. Client > primary FortiGate > secondary FortiGate > primary FortiGate > web server
- C. Client > primary FortiGate > secondary FortiGate > web server
- D. Client > secondary FortiGate > web server

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 2

What three FortiGate components are tested during the hardware test? (Choose three.)

- A. CPU
- B. Administrative access
- C. HA heartbeat
- D. Hard disk
- E. Network interfaces

**Correct Answer: ADE**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 3**

Consider a new IPsec deployment with the following criteria:

- All satellite offices must connect to the two HQ sites.
- The satellite offices do not need to communicate directly with other satellite offices.
- Backup VPN is not required.
- The design should minimize the number of tunnels being configured.

Which topology should you use to satisfy all of the requirements?

- A. Partial mesh
- B. Redundant
- C. Full mesh
- D. Hub-and-spoke

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 4**

Refer to the exhibit.


You are configuring the root FortiGate to implement the Security Fabric. You are configuring port10 to communicate with a downstream FortiGate. The exhibit shows the default **Edit Interface**.



Edit Interface


Interface Name
port10(00:0C:29:0F:A9:F9)

Alias

Link Status
Up 

Type
Physical Interface

Tags

Role 
Undefined


Add Tag Category


Address


Addressing mode
Manual DHCP One-Arm Sniffer

IP/Network Mask

Administrative Access

IPv4
☐ HTTPS ☐ HTTP  ☐ PING ☐ FMG-Access  
☐ CAPWAP ☐ SSH ☐ SNMP ☐ FTM  
☐ RADIUS Accounting ☐ FortiTelemetry

Receive LLDP 
Use VDOM Setting Enable Disable

Transmit LLDP 
Use VDOM Setting Enable Disable

DHCP Server

Networked Devices

Device Detection

When configuring the root FortiGate to communicate with a downstream FortiGate, which two settings must you configure? (Choose two.)

- A. Enable **Device Detection** B.
- Administrative Access: FortiTelemetry.**
- C. **IP/Network Mask.**
- D. **Role: Security Fabric.**

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 5**

Which two statements about NTLM authentication are correct? (Choose two.)

- A. It requires DC agents on every domain controller when used in multidomain environments.
- B. It is useful when users log in to DCs that are not monitored by a collector agent.
- C. It requires NTLM-enabled web browsers.
- D. It takes over as the primary authentication method when configured alongside FSSO.

**Correct Answer:** BC

**Section:** (none)

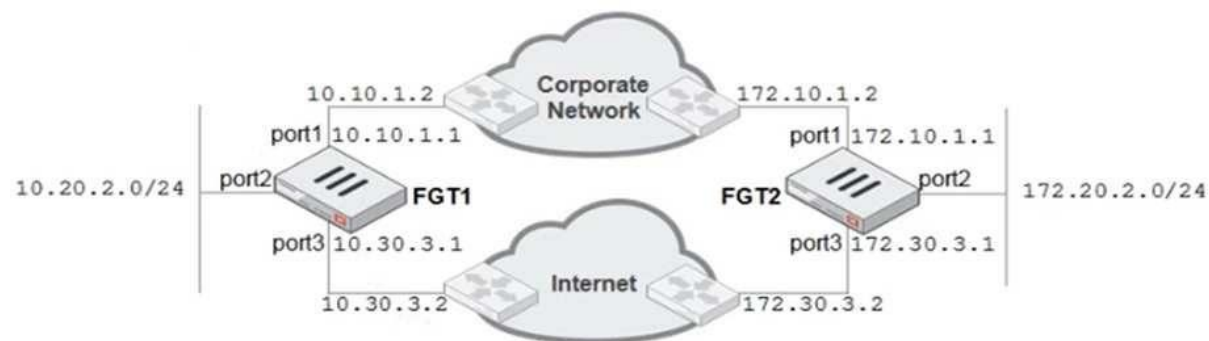
**Explanation**

**Explanation/Reference:**

Reference: <https://www.fortinetguru.com/2016/07/configuring-authenticated-access/12/>

#### **QUESTION 6**

Refer to the exhibit.



A firewall administrator must configure equal cost multipath (ECMP) routing on FGT1 to ensure both port1 and port3 links are used, at the same time, for all traffic destined for 172.20.2.0/24.

Given the network diagram shown in the exhibit, which two static routes will satisfy this requirement on FGT1? (Choose two.)

- A. 172.20.2.0/24 [1/0] via 10.10.1.2, port1 [0/0]
- B. 172.20.2.0/24 [25/0] via 10.30.3.2, port3 [5/0]
- C. 172.20.2.0/24 [25/0] via 10.10.1.2, port1 [5/0]
- D. 172.20.2.0/24 [1/150] via 10.30.3.2, port3 [10/0]

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 7

Refer to the exhibit.

```
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0: IKEv1 exchange=Identity Protection id=4497f0b077c742b5/0000000000000000 len=296
ike 0:4497f0b077c742b5/0000000000000000:8: responder: main mode get 1st message...
...
ike 0:4497f0b077c742b5/0000000000000000:8: SA proposal chosen, matched gateway Remote
ike 0: found Remote 172.20.186.222 2 -> 172.20.187.114:500
...
ike 0:Remote:8: sent IKE msg (ident_r1send): 172.20.186.222:500->172.20.187.114:500, len=160
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder:main mode get 2nd message...
....
ike 0:Remote:8: sent IKE msg (ident_r2send): 172.20.186.222:500->172.20.187.114:500, len=292
ike 0:Remote:8: ISAKMP SA 4497f0b077c742b5/fbbb59b259a0fc3e key 24:DCD18FBE7CFA138E27B06F
ike 0: comes 172.20.187.114:500->172.20.186.222:500,ifindex=2....
ike 0:Remote:8: responder: main mode get 3rd message...
...
ike 0:Remote:8: PSK authentication succeeded
ike 0:Remote:8: authentication OK
ike 0:Remote:8: established IKE SA 4497f0b077c742b5/fbbb59b259a0fc3e
```

Given the partial output of an IKE real-time debug shown in the exhibit, which statement about the output is true?

- A. The VPN is configured to use pre-shared key authentication.
- B. Extended authentication (XAuth) was successful.
- C. Remote is the host name of the remote IPsec peer.
- D. Phase 1 went down.



**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 8

An administrator needs to create an SSL-VPN connection for accessing an internal server using the bookmark, Port Forward.

Which step must the administrator take to successfully achieve this configuration?

- A. Configure an SSL VPN realm for clients to use the Port Forward bookmark.
- B. Configure the client application to forward IP traffic through FortiClient.
- C. Configure the virtual IP address to be assigned to the SSL VPN users.
- D. Configure the client application to forward IP traffic to a Java applet proxy.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 9**

Which two static routes are not maintained in the routing table? (Choose two.)

- A. Dynamic routes
- B. Policy routes
- C. Named Address routes
- D. ISDB routes

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://help.fortinet.com/fadc/4-8-0/olh/Content/FortiADC/handbook/routing-static.htm>

#### **QUESTION 10**

An administrator wants to configure a FortiGate as a DNS server. FortiGate must use a DNS database first, and then relay all irresolvable queries to an external DNS server. Which DNS method must you use?

- A. Recursive
- B. Non-recursive
- C. Forward to primary and secondary DNS
- D. Forward to system DNS

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 11**

Refer to the exhibit.



```
id=2 line=4677 msg= "vd-root received a packet (proto=6, 66.171.121.44:80 ->10.200.1.1:49886) from port1  
flag [S.], seq 3567496940, ack 2176715502, win 5840"  
id=2 line=4739 msg= "Find an existing session, id-00007fc0, reply direction"  
id=2 line=2733 msg= "DNAT 10.200.1.1:49886 -> 10.0.1.10:49886"  
id=2 line=2582 msg= "find a route: flag=00000000 gw-10.0.1.10 via port3"
```

The exhibit shows the output from a debug flow.

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

- A. The packet was allowed by the firewall policy with the ID 00007fc0.
- B. The source IP address of the packet was translated to 10.0.1.10.
- C. FortiGate received a TCP SYN/ACK packet.
- D. FortiGate routed the packet through port3.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**



## QUESTION 12

What is required to create an inter-VDOM link between two VDOMs?

- A. At least one of the VDOMs must operate in NAT mode.
- B. Both VDOMs must operate in NAT mode.
- C. The inspection mode of at least one VDOM must be NGFW policy-based.
- D. The inspection mode of both VDOMs must match.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## QUESTION 13

What FortiGate configuration is required to actively prompt users for credentials?

- A. You must enable one or more protocols that support active authentication on a firewall policy.
- B. You must position the firewall policy for active authentication before a firewall policy for passive authentication
- C. You must assign users to a group for active authentication
- D. You must enable the **Authentication** setting on the firewall policy

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 14

NGFW mode allows policy-based configuration for most inspection rules.

Which security profile configuration does not change when you enable policy-based inspection?

- A. Application control
- B. Web filtering
- C. Web proxy
- D. Antivirus



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 15

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

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

**Correct Answer:** BC

**Section: (none)**

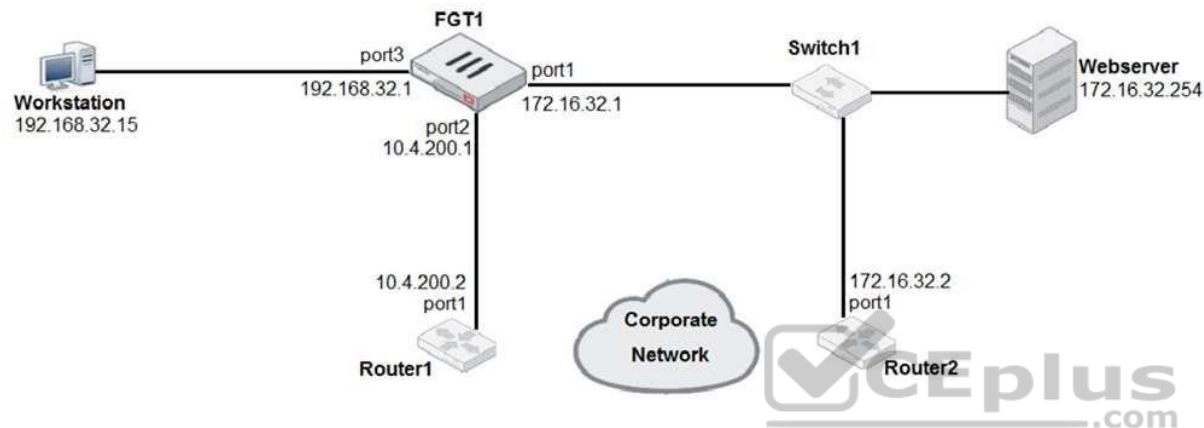
**Explanation**

**Explanation/Reference:**

Reference: [https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA\\_operatingFirmUpgd.htm](https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-high-availability-52/HA_operatingFirmUpgd.htm)

### QUESTION 16

Refer to the exhibit.



Given the network diagram shown in the exhibit, which route is the best candidate route for FGT1 to route traffic from the workstation to the webserver?

- A. 172.16.32.0/24 is directly connected, port1
- B. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
- C. 10.4.200.0/30 is directly connected, port2
- D. 0.0.0.0/0 [20/0] via 10.4.200.2, port2

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 17

Which two statements about central NAT are true? (Choose two.)

- A. SNAT using central NAT does not require a central SNAT policy.

- B. Central NAT can be enabled or disabled from the CLI only.
- C. IP pool references must be removed from existing firewall policies, before enabling central NAT.
- D. DNAT using central NAT requires a VIP object as the destination address in a firewall policy.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 18**

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 19**

Refer to the exhibit.



Application Details

Name :

Category :

Technology :

Popularity :

Addicting Games

Game

Browser-Based

☆☆☆☆

Application Control Profile

Categories

▼ All Categories

▼ Business (144, △6)

▼ Collaboration (268, △10)

▼ Game (87)

▼ Mobile (3)

▼ P2P (63)

▼ Remote.Access (84)

▼ Storage.Backup (173, △17)

▼ Video/Audio (160, △14)

▼ Web.Client (23)

▼ Cloud.IT (43)

▼ Email (80, △12)

▼ General.Interest (231, △7)

▼ Network.Service (329)

▼ Proxy (166)

▼ Social.Media (121, △31)

▼ Update (50)

▼ VoIP (24)

▼ Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New

Edit

Delete

Priority	Details	Type	Action
1	Addicting Games	Application	✓ Allow
2	<div>RISK</div> <div> <div></div> <div></div> <div></div> <div></div> </div>	Filter	✗ Block

A user located behind the FortiGate device is trying to go to <http://www.addictinggames.com> (**Addicting.Games**). The exhibit shows the application detains and application control profile.

Based on this configuration, which statement is true?

- A. **Addicting.Games** will be blocked, based on the **Filter Overrides** configuration.
- B. **Addicting.Games** will be allowed only if the **Filter Overrides** action is set to **Learn**.
- C. **Addicting.Games** will be allowed, based on the **Categories** configuration.
- D. **Addicting.Games** will be allowed, based on the **Application Overrides** configuration.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 20

Refer to the exhibit.

```
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
```



The exhibit shows a FortiGate configuration.



<https://vceplus.com/>

How does 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.

**Correct Answer:** D

**Section:** (none)

**Explanation**



**Explanation/Reference:**

#### QUESTION 21

Which statement about the IP authentication header (AH) used by IPsec is true?

- A. AH does not support perfect forward secrecy.
- B. AH provides strong data integrity but weak encryption.
- C. AH provides data integrity but no encryption.
- D. AH does not provide any data integrity or encryption.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 22**

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

- A. IPSec tunnels are negotiated dynamically between spokes.
- B. ADVPN is supported only with IKEv2.
- C. It recommends the use of dynamic routing protocols, so that spokes can learn the routes to other 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.

**Correct Answer:** AC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

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



**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 24**

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
config system global
set block-session-timer 30
end
```



What are the two results of this configuration? (Choose two.)

- A. Device detection on all interfaces is enforced for 30 minutes.
- B. Denied users are blocked for 30 minutes.
- C. A session for denied traffic is created.
- D. The number of logs generated by denied traffic is reduced.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328>

## QUESTION 25

Refer to the exhibit.

```
date=2017-08-31 time=12:50:06 logid=0316013057 type=utm subtype=webfilter eventtype=ftgd_blk  
level=warning vd=root policyid=1 sessionid=149645 user= "" srcip=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 reqtype=direct url= "/" sentbyte=286  
rcvdbyte=0 direction=outgoing msg= "URL belongs to a category with warnings enabled"  
method=dcmain cat=20 catdesc= "Games" crscore=30 crlevel=high
```

The exhibit shows a web filtering log.

Which statement about the log message is true?

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

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 26**

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

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 27**

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.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 28**

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 192.168.1.0/24 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. 192.168.0.0/8
- C. 192.168.2.0/24
- D. 192.168.3.0/24



**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 29**

Refer to the exhibits.

## IPS Sensor

Edit IPS Sensor WINDOWS\_SERVER [View IPS Signatures]

Name:  [View IPS Signatures]

Comments:

IPS Signatures:

[+ Add Signatures](#) [Delete](#) [Edit IP Exceptions](#)

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
SMTPLoginBruteForce		High	Server	TCP_SMT	All	Block	<input checked="" type="checkbox"/>

IPS Filters:

[+ Add Filter](#) [Edit Filter](#) [Delete](#)

Filter Details	Action	Packet Logging
Location: server Protocol: SMTP	Block	<input checked="" type="checkbox"/>

Rate Based Signatures

Enable	Signature	Threshold	Duration(seconds)	Track By	Action	Block Duration(minutes)
<input checked="" type="checkbox"/>	IMAPLoginBruteForce	60	10	Source IP	Block	None

[Apply](#)

## DoS Policy

Incoming Interface:

Source Address:  [+](#) [X](#)

Destination Address:  [+](#) [X](#)

Services:  [+](#) [X](#)

### L3 Anomalies

Name	Status	Logging	Pass	Block	Action	Threshold
ip_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Pass	Block		60
ip_dst_session	<input type="checkbox"/>	<input type="checkbox"/>	Pass	Block		5000

The exhibits show the IPS sensor and DoS policy configuration.

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

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

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 30

Refer to the exhibit.

▼ Status	▼ Name	▼ VLAN ID	▼ Type	IP/Netmask
Physical(12)				
	port1		Physical Interface	10.200.1.1 255.255.255.0
	port1-VLAN1	1	VLAN	10.200.5.1 255.255.255.0
	port1-VLAN10	10	VLAN	10.0.10.1 255.255.255.0
	port2		Physical Interface	10.200.2.1 255.255.255.0
	port2-VLAN1	1	VLAN	10.0.5.1 255.255.255.0
	port2-VLAN10	10	VLAN	10.0.20.254 255.255.255.0
	port3		Physical Interface	10.0.1.254 255.255.255.0

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

- A. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.
- B. Broadcast traffic received on port1-VLAN10 will not be forwarded to port2-VLAN10
- C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
- D. port1-VLAN1 is the native VLAN for the port1 physical interface.

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 31**

An administrator observes that the `port1` interface *cannot* be configured with an IP address.

What are three possible reasons for this? (Choose three.)

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

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

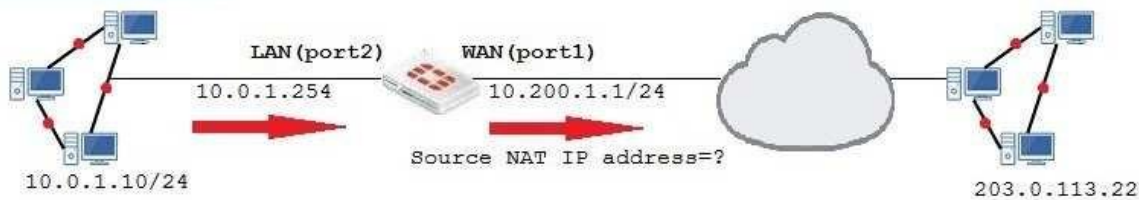
**Explanation/Reference:**




**QUESTION 32**

Refer to the exhibits.

**Network Diagram**



## Virtual IP

Name	<input type="text" value="VIP"/>	
Comments	<input type="text"/>	
Color	 <input type="button" value="Change"/>	
Network		
Interface	<input type="text" value="WAN (port1)"/>	
Type	Static NAT	
External IP Address/Range	<input type="text" value="10.200.1.10"/> - <input type="text" value="10.200.1.10"/>	
Mapped IP Address/Range	<input type="text" value="10.0.1.10"/> - <input type="text" value="10.0.1.10"/>	
Optional Filters	<input type="checkbox"/>	
Port Forwarding	<input type="checkbox"/>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

Firewall Policies							
ID	Name	Source	Destination	Schedule	Service	Action	NAT
LAN(port2)→ WAN(port1) 1							
1	Full_Access	all	all	always	ALL	✓ ACCEPT	✓ Enabled
WAN(port1)→ LAN(port2) 1							
2	WebServer	all	VIP	always	ALL	✓ ACCEPT	✗ Disabled

The exhibits contain a network diagram and virtual IP and firewall policy configuration.

The WAN (port1) interface has the IP address 10.200.1.1/24. The LAN (port2) interface has the IP address 10.0.1.254/24.

The first firewall policy has NAT enabled on the outgoing interface address. 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 10.0.1.10/32?

- A. Any available IP address in the WAN (port1) subnet 10.200.1.0/24
- B. 10.200.1.10
- C. 10.200.1.1
- D. 10.0.1.254

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 33

Refer to the exhibit.



### FortiGate Configuration

```
config system global  
  
    set av-failopen pass  
  
end
```

### Debug command output

```
# diagnose hardware sysinfo conserve  
  
memory conserve mode: on  
  
total RAM: 3040 MB  
  
memory used: 2948 MB 97% of total RAM  
memory freeable: 92 MB 3% of total RAM  
memory used + freeable threshold extreme: 2887 MB 95% of total RAM  
memory used threshold red: 2675 MB 88% of total RAM  
memory used threshold green: 2492 MB 82% of total RAM
```

The exhibit shows FortiGate configuration and the output of the debug command.

Based on the diagnostic output, how is the FortiGate handling the traffic for new sessions that require proxy based inspection?

- A. It is allowed, but with no inspection.
- B. It is allowed and inspected, as long as the only inspection required is antivirus.
- C. It is dropped.
- D. It is allowed and inspected, as long as the inspection is flow based.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 34**

Which two SD-WAN load balancing methods use interface weight value to distribute traffic?

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

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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



<https://vceplus.com/>