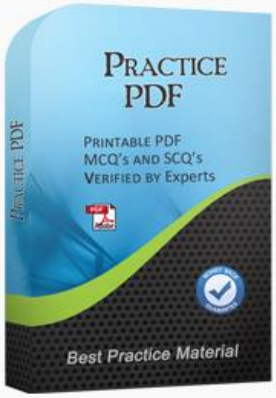
ActualtestsQuiz

ActualtestsQuiz

- Online Tool, Convenient, easy to study.
- Instant Online Access
- Supports All Web Browsers
- Practice Online Anytime
- Test History and Performance Review
- Supports Windows / Mac / Android / iOS, etc.

- Installable Software Application
- Simulates Real Exam Environment
- Builds Exam Confidence
- Supports MS Operating System
- Two Modes For Practice
- Practice Offline Anytime



- Printable PDF Format
- Prepared by IT Experts
- Instant Access to Download
- Study Anywhere, Anytime
- 365 Days Free Updates
- Free PDF Demo Available

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Exam : **NSE4_FGT-7.2**

Title : Fortinet NSE 4 - FortiOS 7.2

Vendor : Fortinet

Version : DEMO

QUESTION NO: 1
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)
A. diagnose sys top
B. execute ping
C. execute traceroute
D. diagnose sniffer packet any
E. get system arp
Answer: B,C,D

QUESTION NO: 2
Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)
A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.
C. Highest to lowest priority defined in the firewall policy.
D. Services defined in the firewall policy.
E. Lowest to highest policy ID number.
Answer: A,B,D
Explanation:
When a packet arrives, how does FortiGate find a matching policy? Each policy has match criteria, which you can define using the following objects:
* Incoming Interface
* Outgoing Interface
* Source: IP address, user, internet services
* Destination: IP address or internet services
* Service: IP protocol and port number
* Schedule: Applies during configured times

QUESTION NO: 3
Refer to the exhibits.

Exhibit A

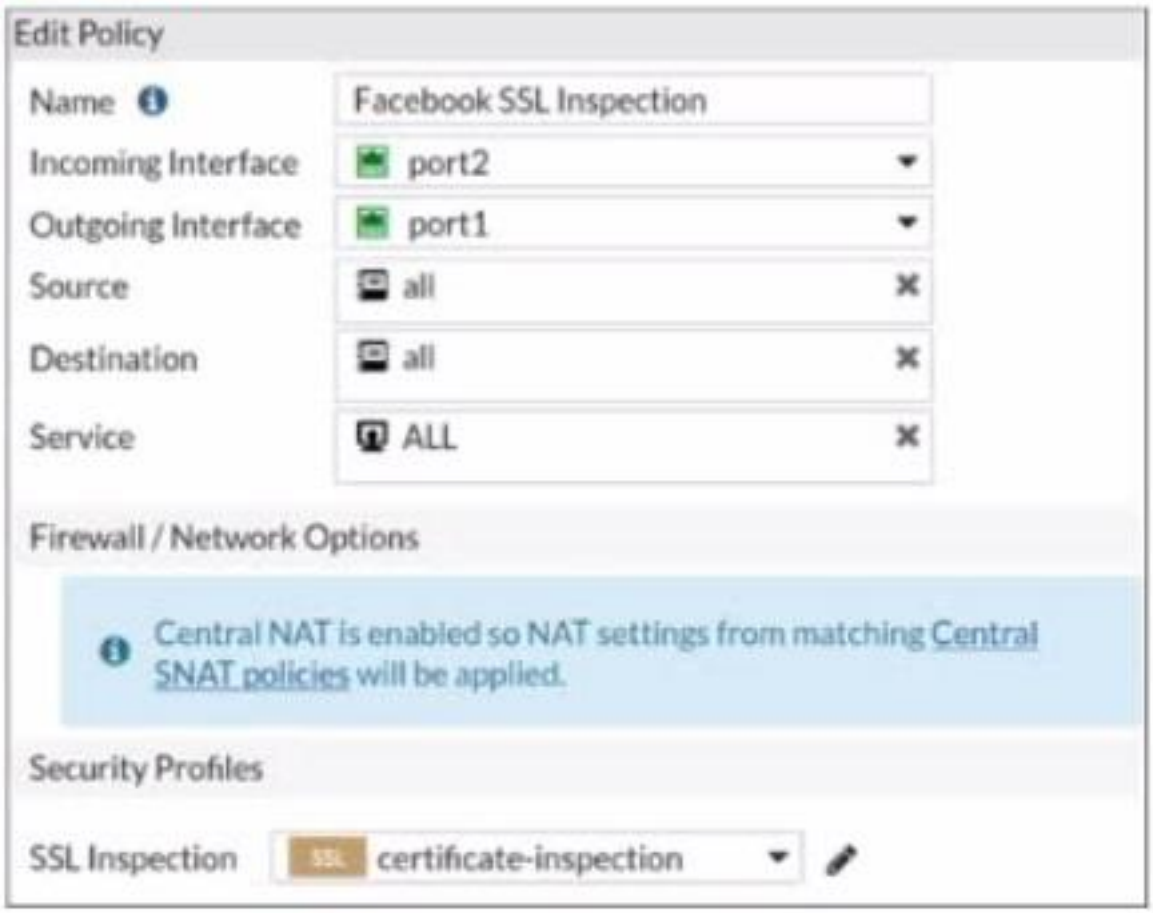

Edit Policy
Name
Facebook SSL Inspection
Incoming Interface
port2
Outgoing Interface
port1
Source
all
Destination
all
Service
ALL
Firewall / Network Options
Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.
Security Profiles
SSL Inspection
certificate-inspection

Exhibit B

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.

QUESTION NO: 4
Refer to the exhibits.

Exhibit A shows a network diagram. Exhibit B shows the firewall policy configuration and a VIP object 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.

Exhibit A | Exhibit B

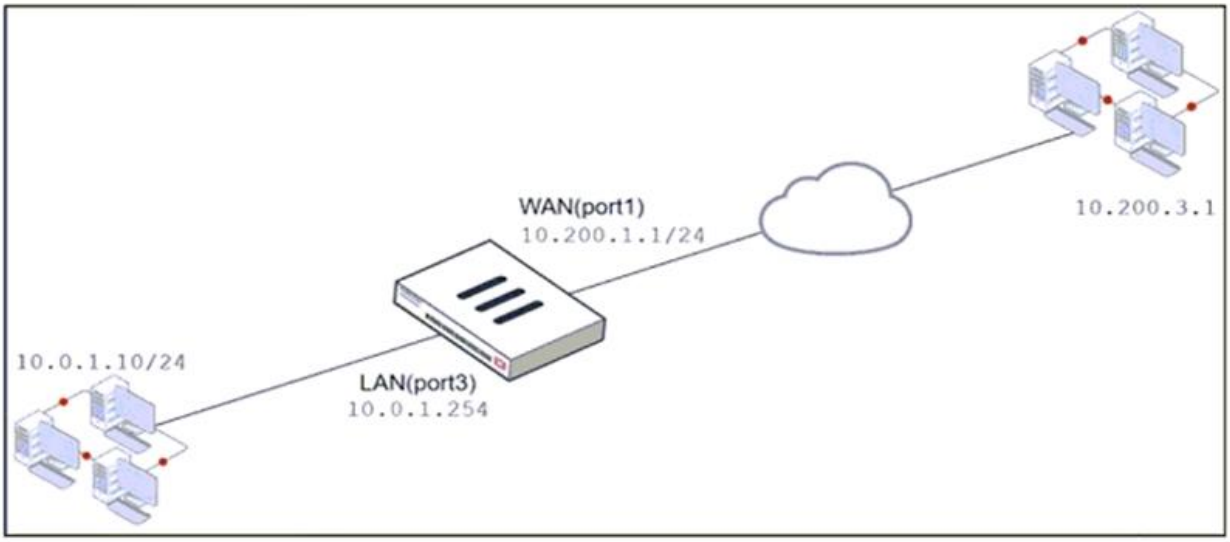


Exhibit A | Exhibit B

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
WebServer	WAN (port1)	LAN (port3)	all	VIP	always	ALL	ACCEPT	Enabled

Edit Virtual IP

VIP type	IPv4
Name	VIP
Comments	Write a comment... 0/255
Color	Change
Network	
Interface	WAN (port1)
Type	Static NAT
External IP address/range	10.200.1.10
Map to	
IPv4 address/range	10.0.1.10
Optional Filters	
Port Forwarding	
Protocol	TCP UDP SCTP ICMP
Port Mapping Type	One to one Many to many
External service port	10443
Map to IPv4 port	443

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the

source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

A. 10.0.1.254, 10.0.1.10, and 443, respectively

B. 10.0.1.254, 10.200.1.10, and 443, respectively

C. 10.200.3.1, 10.0.1.10, and 443, respectively

D. 10.0.1.254, 10.0.1.10, and 10443, respectively

Answer: C

Explanation:

The host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, which is the external IP address of the VIP object named VIP in Exhibit B1. The VIP object maps the external IP address and port to the internal IP address and port of the server 10.0.1.10 and 443, respectively1. The VIP object also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.

The firewall policy ID 1 in Exhibit B allows traffic from WAN (port1) to LAN (port3) with the destination address of VIP and the service of HTTPS1. The policy also enables NAT, which means that the source address of the packet will be translated to the IP address of the outgoing interface2.

Therefore, after FortiGate forwards the packet to the destination, the source address, destination address, and destination port of the packet will be 10.200.3.1, 10.0.1.10, and 443, respectively.

You can find more information about VIP objects and firewall policies in the Fortinet Documentation

QUESTION NO: 5

Refer to the exhibit.

The exhibit shows the output of a diagnose command.

```
# diagnose firewall proute list
list route policy info(vf=root):
id=2130903041(0x7f030001) vwl_service=1(Critical-DIA) vwl_mbr_seq=1 2 dscp_tag=0xff 0xff
flags=0x0 tos=0x00 tos_mask=0x00 protocol=0 sport=0-65535 iif=0 dport=1-65535 path(2)
oif=3(port1) oif=4(port2)
source(1): 10.0.1.0-10.0.1.255
destination wildcard(1): 0.0.0.0/0.0.0.0
internet service(3): GoToMeeting(4294836966,0,0,0, 16354)
Microsoft.Office.365.Portal(4294837474,0,0,0, 41468) Salesforce(4294837976,0,0,0, 16920)
hit_count=0 last_used=2022-02-23 05:46:43
```

What does the output reveal about the policy route?

A. It is an ISDB route in policy route.

B. It is a regular policy route.

C. It is an ISDB policy route with an SDWAN rule.

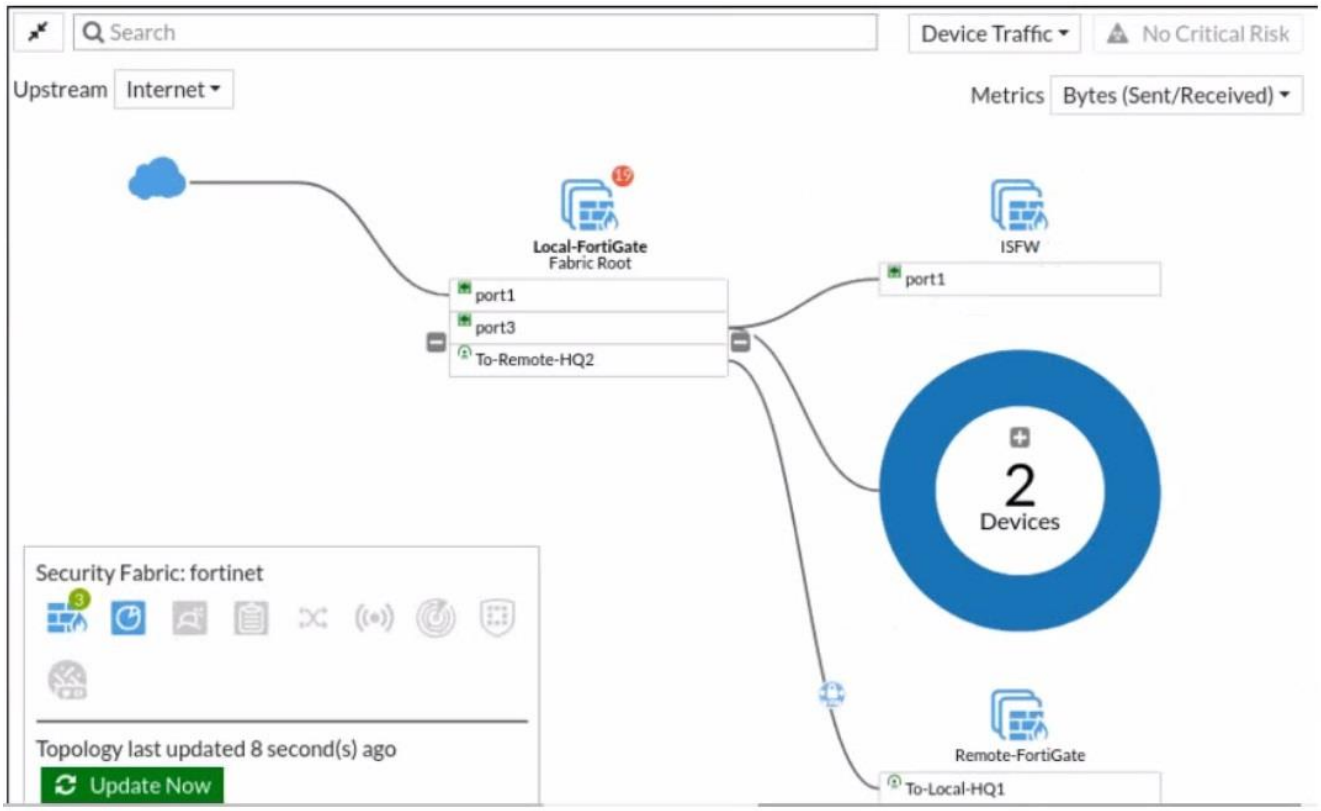
D. It is an SDWAN rule in policy route.

Answer: D

Explanation:

FortiGate Infrastructure 7.2 Study Guide (p.59): "ISDB routes and SD-WAN rules are assigned an ID higher than 65535. However, SD-WAN rule entries include the vwl_service field, and ISDB route entries don't."

QUESTION NO: 6
Refer to the exhibit.



Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)
A. There are five devices that are part of the security fabric.
B. Device detection is disabled on all FortiGate devices.
C. This security fabric topology is a logical topology view.
D. There are 19 security recommendations for the security fabric.
Answer: C,D
Reference:
https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results
https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology

QUESTION NO: 7
What are two functions of the ZTNA rule? (Choose two.)
A. It redirects the client request to the access proxy.
B. It applies security profiles to protect traffic.
C. It defines the access proxy.
D. It enforces access control.
Answer: B,D

Explanation:
A ZTNA rule is a policy that enforces access control and applies security profiles to protect traffic between the client and the access proxy1. A ZTNA rule defines the following parameters1:
Incoming interface: The interface that receives the client request.
Source: The address and user group of the client.
ZTNA tag: The tag that identifies the domain that the client belongs to.
ZTNA server: The server that hosts the access proxy.
Destination: The address of the application that the client wants to access.
Action: The action to take for the traffic that matches the rule. It can be accept, deny, or redirect.
Security profiles: The security features to apply to the traffic, such as antivirus, web filter, application control, and so on.
A ZTNA rule does not redirect the client request to the access proxy. That is the function of a policy route that matches the ZTNA tag and sends the traffic to the ZTNA server2.
A ZTNA rule does not define the access proxy. That is done by creating a ZTNA server object that specifies the IP address, port, and certificate of the access proxy3.
FortiGate Infrastructure 7.2 Study Guide (p.177): "A ZTNA rule is a proxy policy used to enforce access control. You can define ZTNA tags or tag groups to enforce zero-trust role-based access. To create a rule, type a rule name, and add IP addresses and ZTNA tags or tag groups that are allowed or blocked access. You also select the ZTNA server as the destination. You can also apply security profiles to protect this traffic."

QUESTION NO: 8
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: A,C
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.
Reference:
https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol FortiGate Infrastructure 7.2 Study Guide (p.292): "FortiGate HA uses the

Fortinet-proprietary FortiGate Clustering Protocol (FGCP) to discover members, elect the primary FortiGate, synchronize data among members, and monitor the health of members. To discover and monitor members, the members broadcast heartbeat packets over all configured heartbeat interfaces."

QUESTION NO: 9
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, what are two requirements for the VLAN ID? (Choose two.)
A. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.
B. The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs.
C. The two VLAN subinterfaces must have different VLAN IDs.
D. The two VLAN subinterfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
Answer: B,C
Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Note-How-to-use-emac-vlan-to-share-the-same-VLAN/ta-p/192843?externalID=FD43883 When FortiGate is operating in NAT mode, it means that it uses network address translation (NAT) to modify the source or destination IP addresses of the traffic passing through it1. NAT mode allows FortiGate to hide the IP addresses of the internal network from the external network, and to conserve IP addresses by using a single public IP address for multiple private IP addresses1.
A virtual LAN (VLAN) subinterface is a logical interface that allows traffic from different VLANs to enter and exit the FortiGate unit2. A VLAN subinterface is created by adding a VLAN ID to a physical interface or an aggregate interface2. A VLAN ID is a numerical identifier that distinguishes one VLAN from another2.
In this scenario, there are two requirements for the VLAN ID of the VLAN subinterfaces added to the same physical interface:
The two VLAN subinterfaces must have different VLAN IDs. This is because the VLAN ID is used to tag the traffic with the appropriate VLAN information, and to separate the traffic into different VLANs2. If the two VLAN subinterfaces have the same VLAN ID, they will not be able to distinguish the traffic from each other, and they will not be able to forward the traffic to the correct destination.
The two VLAN subinterfaces can have the same VLAN ID, only if they belong to different VDOMs. This is because VDOMs are virtual instances of FortiGate that can have their own interfaces, policies, and routing tables3. Each VDOM operates independently from other VDOMs, and can have its own VLAN subinterfaces with different or identical VLAN IDs3. However, this requires inter-VDOM links to allow traffic between different VDOMs3.

QUESTION NO: 10
What is a reason for triggering IPS fail open?
A. The IPS socket buffer is full and the IPS engine cannot process additional packets.
B. The IPS engine cannot decode a packet.

C. The IPS engine is upgraded.
D. The administrator enabled NTurbo acceleration.
Answer: A

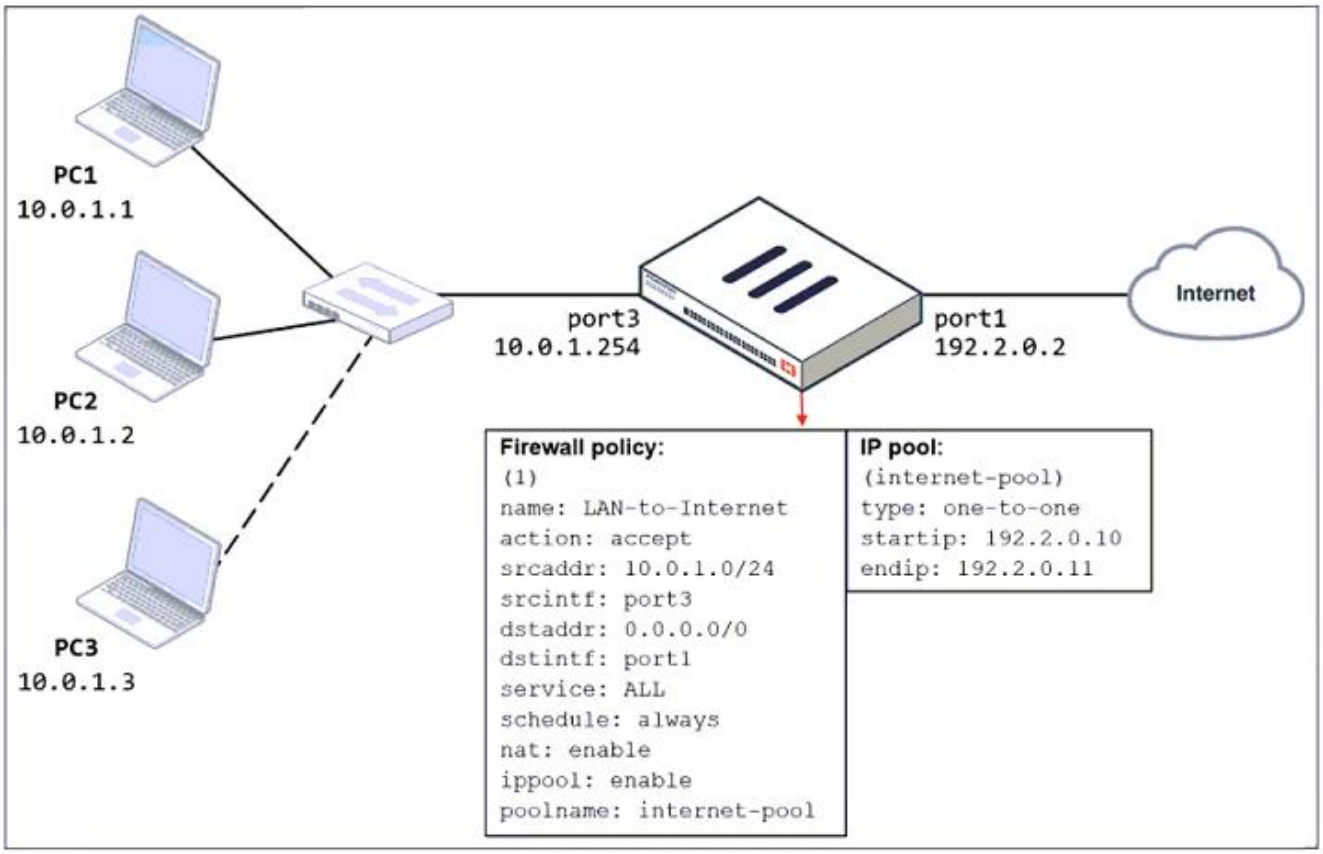
QUESTION NO: 11
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal ?
A. By default, FortiGate uses WINS servers to resolve names.
B. By default, the SSL VPN portal requires the installation of a client's certificate.
C. By default, split tunneling is enabled.
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.
Answer: D

QUESTION NO: 12
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: C,D
Explanation:
Fortigate Infrastructure 7.0 Study Guide P.272-273
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732

QUESTION NO: 13
What are two functions of ZTNA? (Choose two.)
A. ZTNA manages access through the client only.
B. ZTNA manages access for remote users only.
C. ZTNA provides a security posture check.
D. ZTNA provides role-based access.
Answer: C,D
Reference:
ZTNA (Zero Trust Network Access) is a security architecture that is designed to provide secure access to network resources for users, devices, and applications. It is based on the principle of "never trust, always verify," which means that all access to network resources is subject to strict verification and authentication.
Two functions of ZTNA are:
ZTNA provides a security posture check: ZTNA checks the security posture of devices and users that are attempting to access network resources. This can include checks on the device's software and hardware configurations, security settings, and the presence of malware.
ZTNA provides role-based access: ZTNA controls access to network resources based on the role of the user or device. Users and devices are granted access to only those resources that

are necessary for their role, and all other access is denied. This helps to prevent unauthorized access and minimize the risk of data breaches.

QUESTION NO: 14
Refer to the exhibit.



The exhibit shows a diagram of a FortiGate device connected to the network and the firewall policy and IP pool configuration on the FortiGate device.
Two PCS, PCI and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the Intarnet_ Based on the information shown in the exhibit, which three configuration changes should the administrator make to fix the connectivity issue for PC3? (Choose three.)

A. In the IP pool configuration, set type to overload.

B. Configure 192.2. O. 12/24 as the secondary IP address on port1

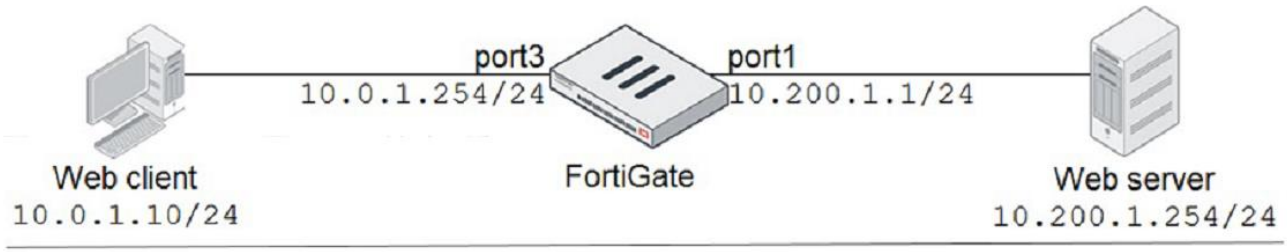
C. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.

D. In the IP pool configuration, set endip to 192.2. O .12

E. In the firewall policy configuration, disable ippool.

Answer: A,D,E

QUESTION NO: 15
Refer to the exhibit.




```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port=80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49256 -> 10.200.1.254.80: syn 868017830
```

In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.

B. Capture the traffic using an external sniffer connected to port1.

C. Execute another sniffer in the FortiGate, this time with the filter host 10.0.1.10€

D. Execute a debug flow.

Answer: D

Explanation:
This solution will help the administrator troubleshoot the problem by tracing the packet flow through the FortiGate device and displaying the details of each step. A debug flow can show the source and destination interfaces, the firewall policy, the routing table, the NAT translation, the security profiles, and the session information of the packet1. A debug flow can also show any errors or anomalies that occur during the packet processing. To execute a debug flow, the administrator can use the diagnose debug flow command in the CLI

QUESTION NO: 16
If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source filed of a firewall policy?

A. IP address

B. Once Internet Service is selected, no other object can be added

C. User or User Group

D. FQDN address

Answer: B

Reference:
https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy

QUESTION NO: 17
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time

B. FortiGuaid update servers
C. Operating mode
D. NGFW mode
Answer: C,D
Explanation:
C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.
D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

QUESTION NO: 18
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)
A. Log downloads from the GUI are limited to the current filter view
B. Log backups from the CLI cannot be restored to another FortiGate.
C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.
Answer: A,B