Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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: ABD

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

NEW QUESTION 2
A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.
What is the reason for the certificate warning errors?

A. The matching firewall policy is set to proxy inspection mode.
B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.
C. The full SSL inspection feature does not have a valid license.
D. The browser does not trust the certificate used by FortiGate for SSL inspection.

Answer: D

Explanation:
FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser."

NEW QUESTION 3
Refer to the exhibit.
A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 status is up, but phase 2 fails to come up.

Based on the phase 2 configuration shown in the exhibit, which configuration change will bring phase 2 up?

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

Answer: B

NEW QUESTION 4
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: BD

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."

NEW QUESTION 5
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: BCD

NEW QUESTION 6
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.
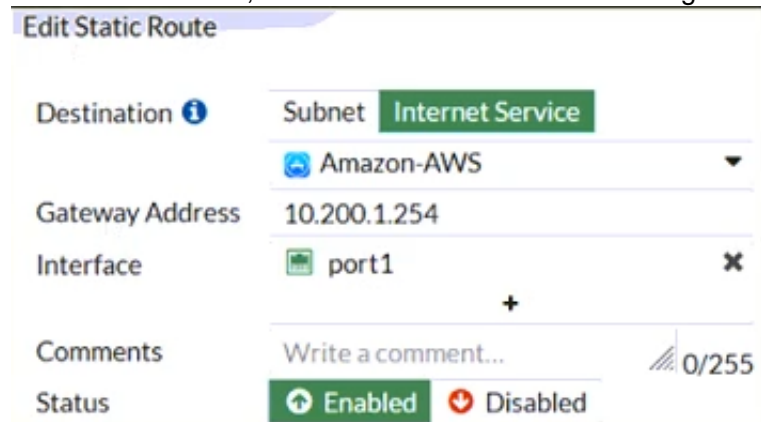C. The issuer must be a public CA.
D. The CA extension must be set to TRUE.

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 7
Refer to the exhibit, which contains a static route configuration. An administrator created a static route for Amazon Web Services.

Which CLI command must the administrator use to view the route?

A. get router info routing-table database
B. diagnose firewall route list
C. get internet-service route list
D. get router info routing-table all

Answer: B

Explanation:

ISDB static route will not create entry directly in routing-table. Reference: https://community.fortinet.com/t5/FortiGate/Technical-Tip-Creating-a-static-route-for-Predefined-Internet/ta-p/1
and here
https://community.fortinet.com/t5/FortiGate/Technical-Tip-Verify-the-matching-policy-route/ta-p/190640
FortiGate Infrastructure 7.2 Study Guide (p.16 and p.59): "Even though they are configured as static routes, ISDB routes are actually policy routes and take precedence over any other routes in the routing table. As such, ISDB routes are added to the policy routing table." "FortiOS maintains a policy route table that you can view by running the diagnose firewall proute list command."

NEW QUESTION 8

A network administrator is troubleshooting an IPsec tunnel between two FortiGate devices. The administrator has determined that phase 1 fails to come up. The administrator has also re-entered the pre-shared key on both FortiGate devices to make sure they match.
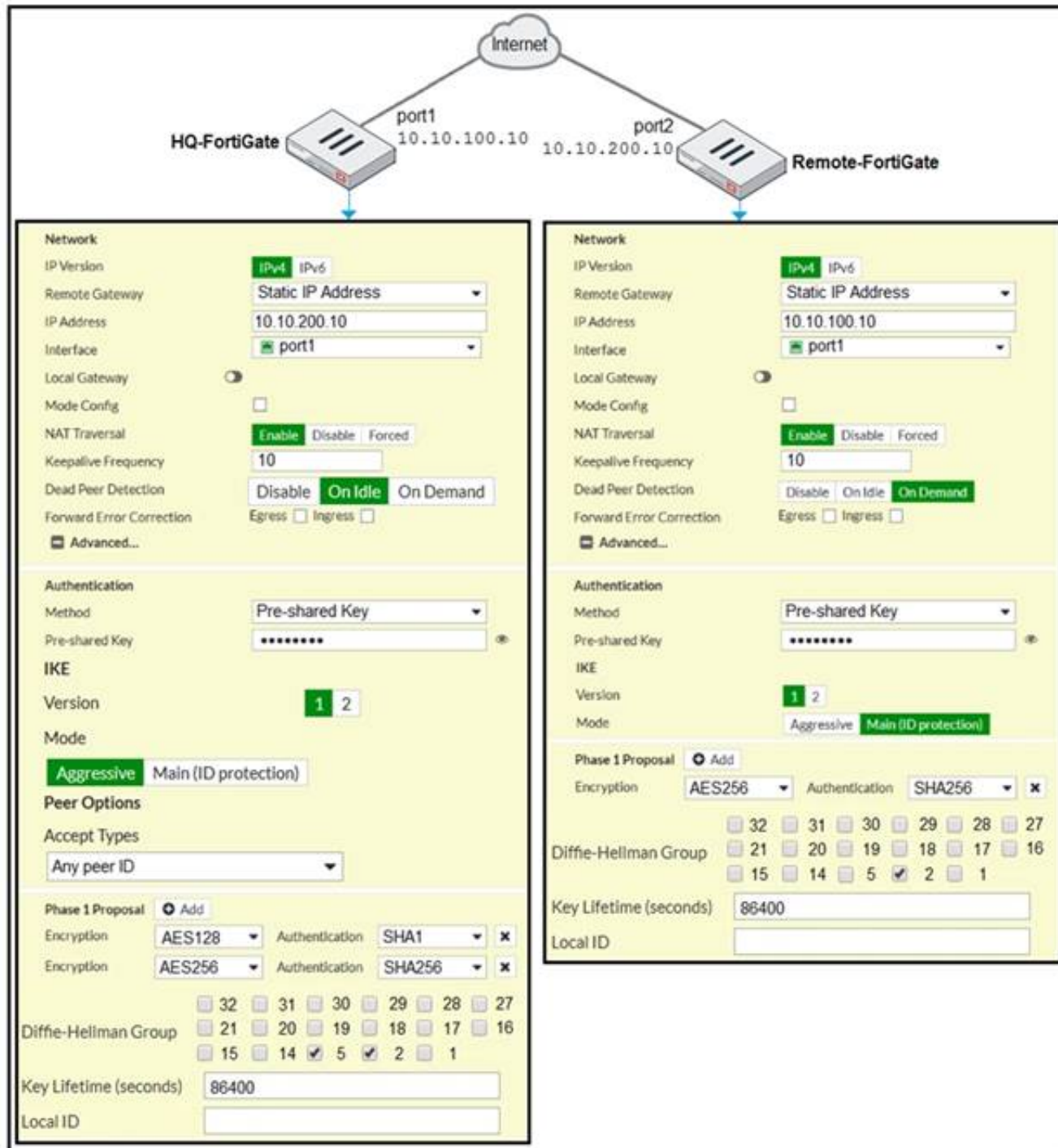
Based on the phase 1 configuration and the diagram shown in the exhibit, which two configuration changes will bring phase 1 up? (Choose two.)

A. On HQ-FortiGate, set IKE mode to Main (ID protection).
B. On both FortiGate devices, set Dead Peer Detection to On Demand.
C. On HQ-FortiGate, disable Diffie-Helman group 2.
D. On Remote-FortiGate, set port2 as Interface.

Answer: AD

Explanation:
"In IKEv1, there are two possible modes in which the IKE SA negotiation can take place: main, and aggressive mode. Settings on both ends must agree; otherwise, phase 1 negotiation fails and both IPsec peers are not able to establish a secure channel."

NEW QUESTION 9
Which two types of traffic are managed only by the management VDOM? (Choose two.)

A. FortiGuard web filter queries
B. PKI
C. Traffic shaping
D. DNS

Answer: AD

NEW QUESTION 10
The IPS engine is used by which three security features? (Choose three.)

A. Antivirus in flow-based inspection

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

Answer: ABC

Explanation:
FortiGate Security 7.2 Study Guide (p.385): "The IPS engine is responsible for most of the features shown in this lesson: IPS and protocol decoders. It's also responsible for application control, flow-based antivirus protection, web filtering, and email filtering."

NEW QUESTION 10
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.
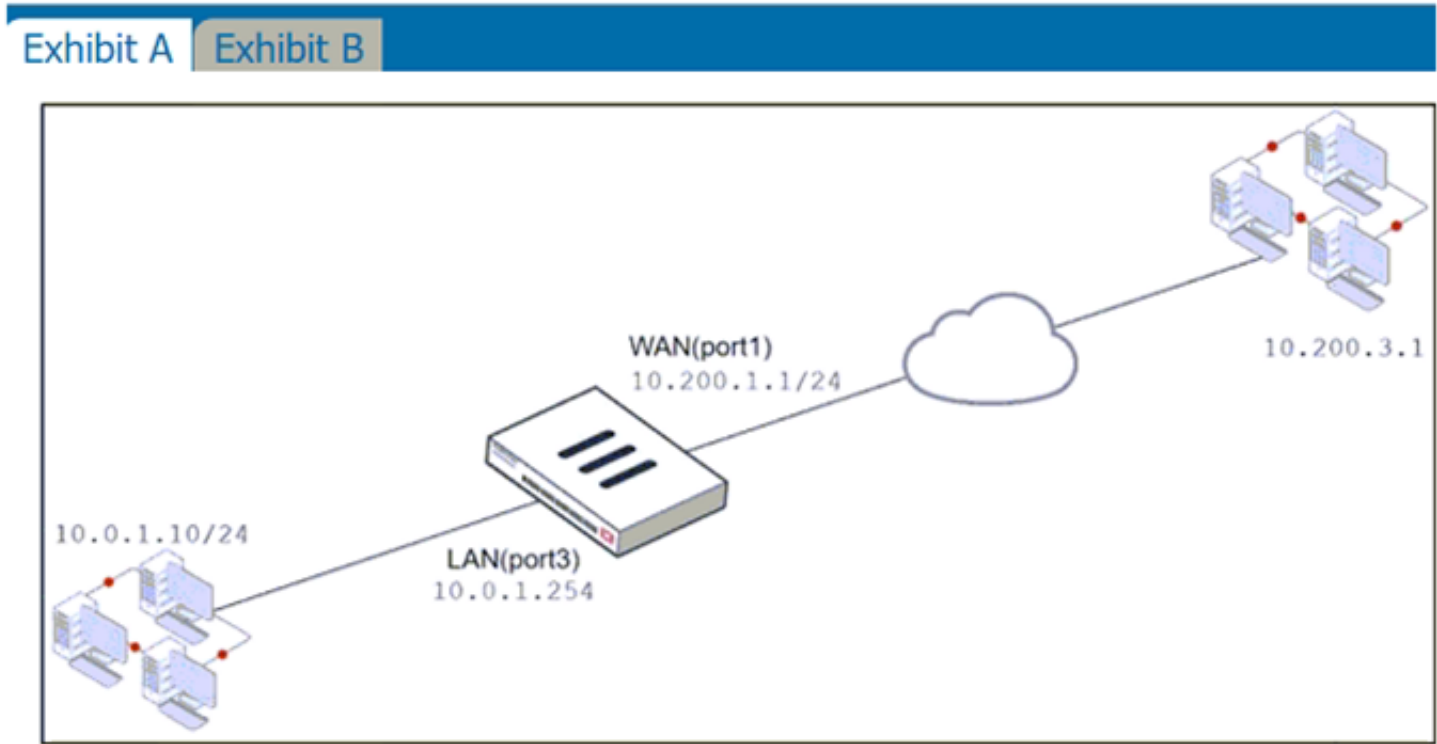

If the host 10.200.3.1 sends a TCP SYN packet on port 10443 to 10.200.1.10, what will the source address, destination address, and destination port of the packet be, after FortiGate forwards the packet to the destination?

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

NEW QUESTION 13

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.
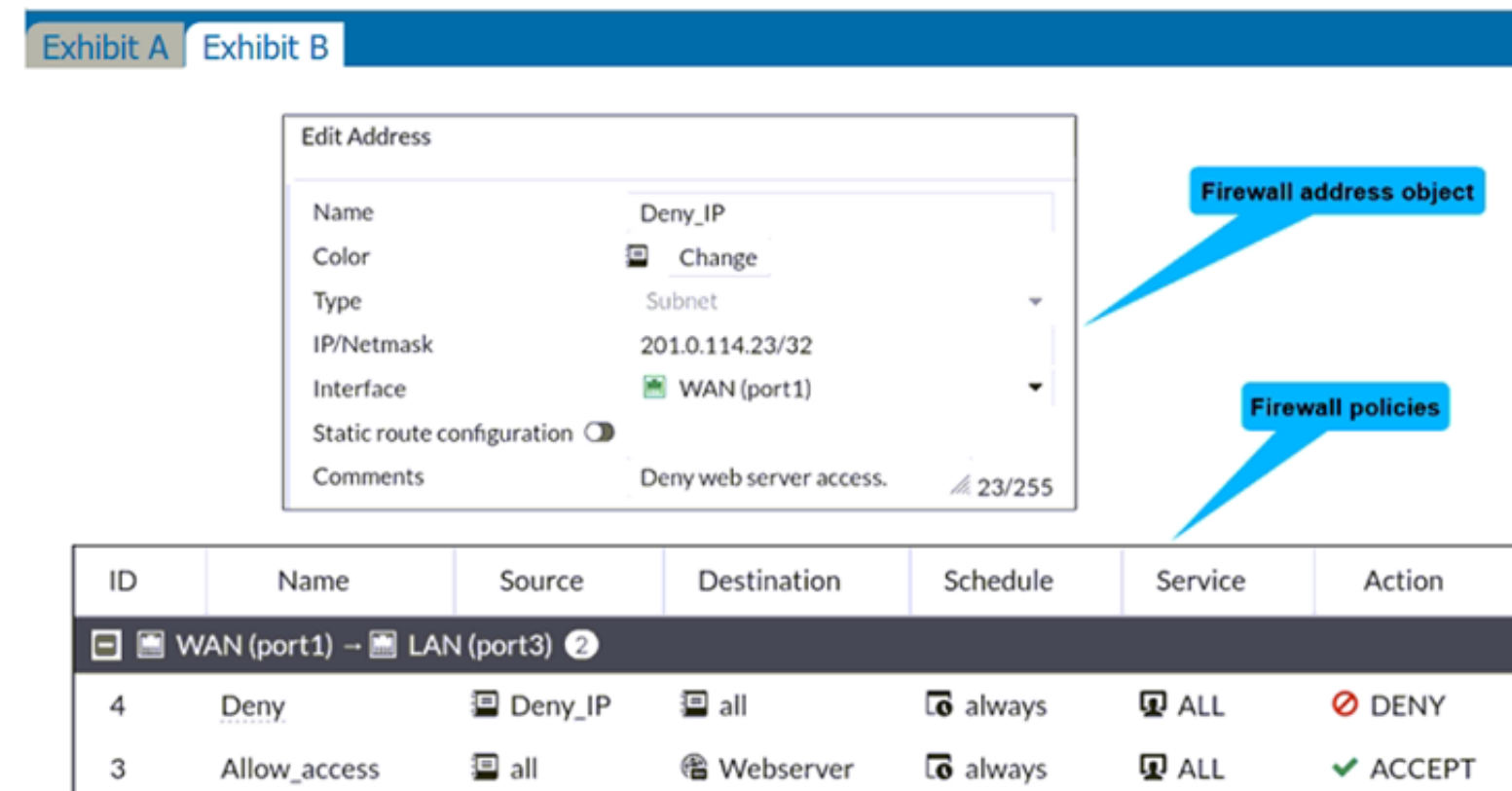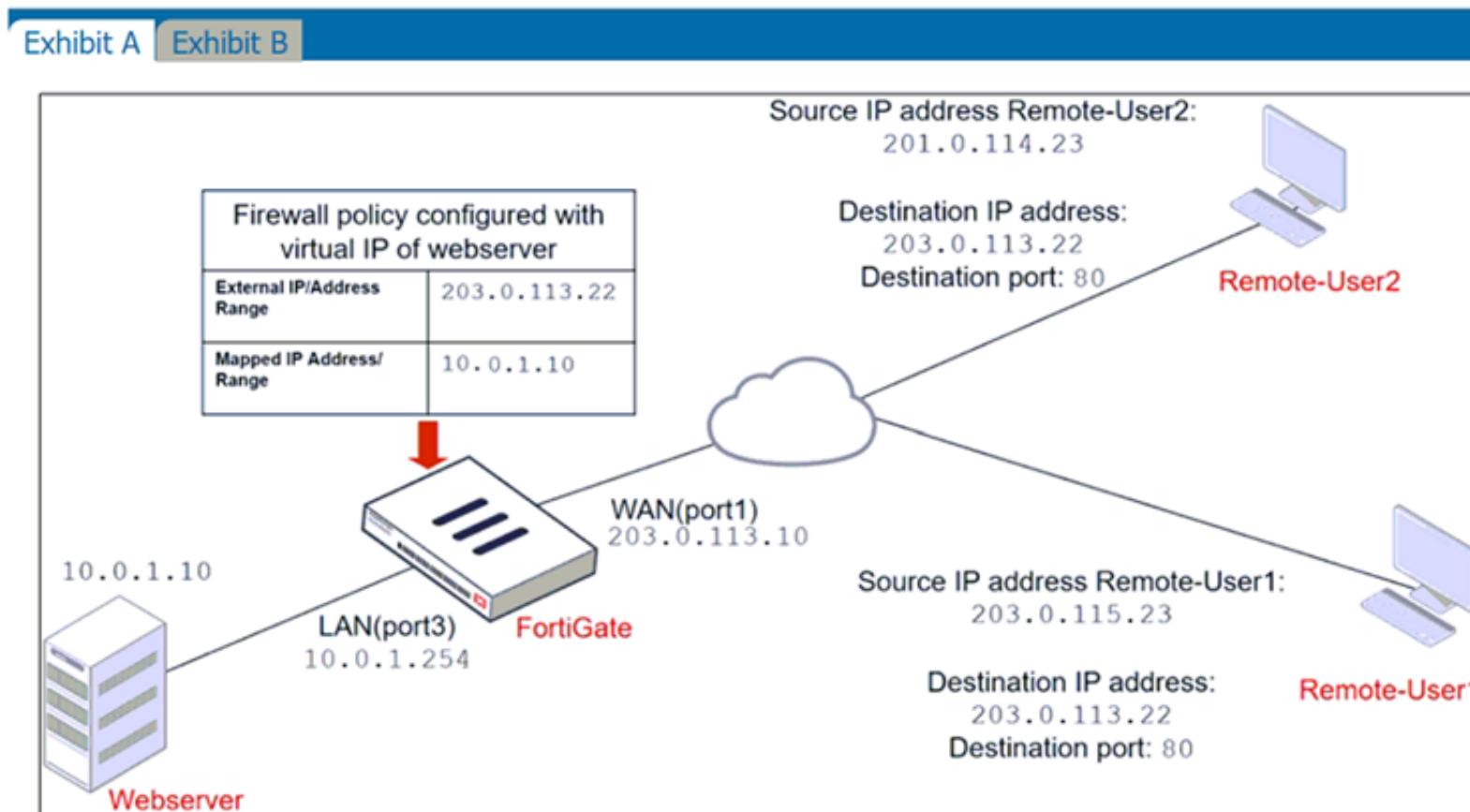

In this scenario, which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

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: BC

Explanation:

https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firewall-does-not-block-incoming-WAN-to-LAN/ta The exhibits show a network diagram and firewall configurations for a FortiGate unit that has two policies:

Allow_access and Deny. The Allow_access policy allows traffic from the WAN (port1) interface to the LAN (port3) interface with the destination address of VIP and the service of HTTPS. The VIP object maps the external IP address 10.200.1.10 and port 10443 to the internal IP address 10.0.1.10 and port 443 of the

Webserver. The Deny policy denies traffic from the WAN (port1) interface to the LAN (port3) interface with the source address of Deny_IP and the destination address of All.

In this scenario, the administrator wants to deny Webserver access for Remote-User2, who has the IP address 10.200.3.2 , which is included in the Deny_IP address object. Remote-User1, who has the IP address 10.200.3.1, must be able to access the Webserver.

To achieve this goal, the administrator can make two changes to deny Webserver access for Remote-User2:

> Set the Destination address as Webserver in the Deny policy. This will make the Deny policy more specific and match only the traffic that is destined for the Webserver's internal IP address, instead of any destination address.

> Enable match-vip in the Deny policy. This will make the Deny policy apply to traffic that matches a VIP object, instead of ignoring it1. This way, the Deny policy will block Remote-User2's traffic that uses the VIP object's external IP address and port.

NEW QUESTION 16
Which scanning technique on FortiGate can be enabled only on the CLI?

A. Heuristics scan
B. Trojan scan
C. Antivirus scan
D. Ransomware scan

Answer: A

NEW QUESTION 18
What are two characteristics of FortiGate HA cluster virtual IP addresses? (Choose two.)

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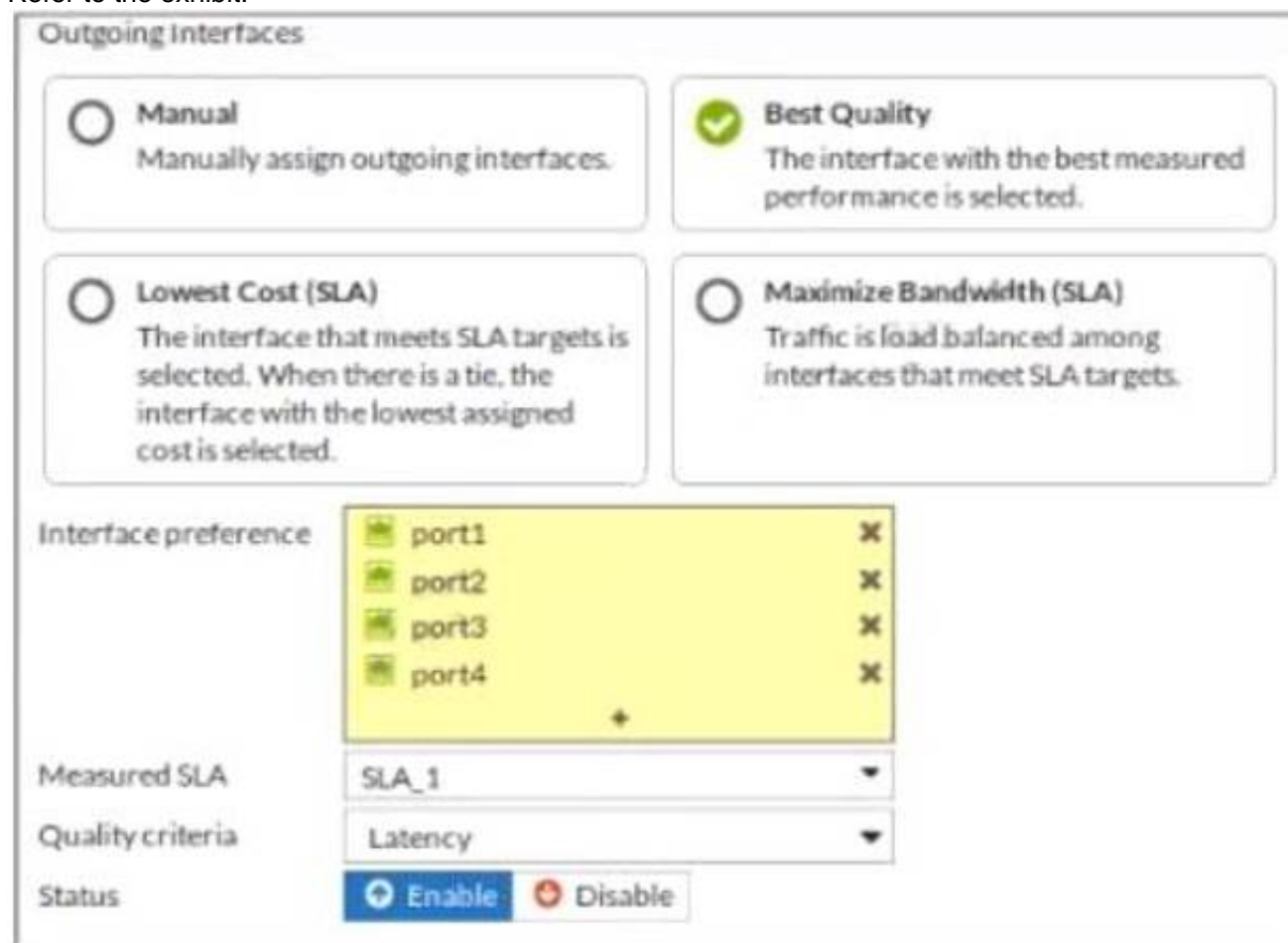
Answer: AD

Explanation:
Fortigate Infrastructure 7.2 Study Guide page 301 FortiGate Infrastructure 7.2 Study Guide (p.301):
"FGCP automatically assigns the heartbeat IP addresses based on the serial number of each device. The IP address 169.254.0.1 is assigned to the device with the highest serial number."
"A change in the heartbeat IP addresses may happen when a FortiGate device joins or leaves the cluster." "The HA cluster uses the heartbeat IP addresses to distinguish the cluster members and synchronize data." https://networkinterview.com/fortigate-ha-high-availability/

NEW QUESTION 20
Refer to the exhibit.

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: D

Explanation:
Port 1 shows the lowest latency.

NEW QUESTION 21
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
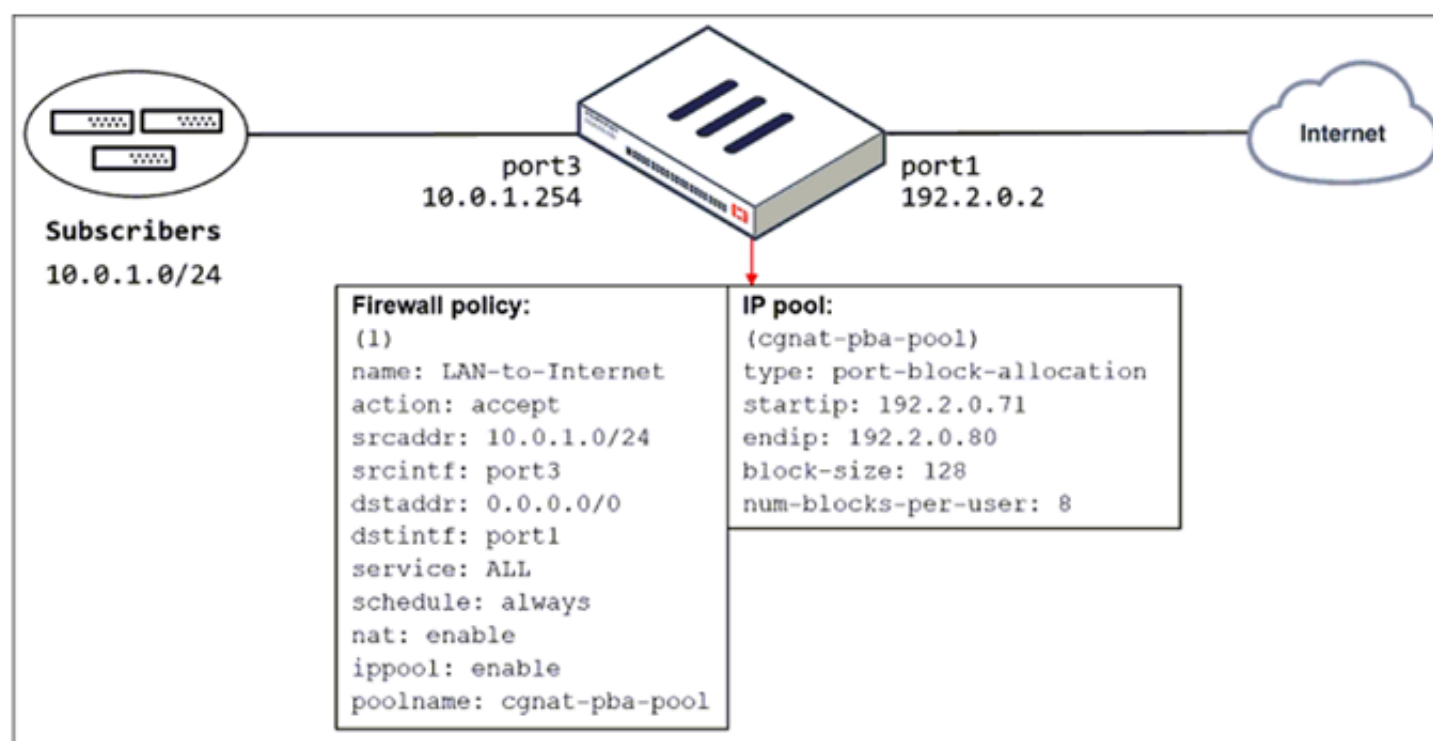
Answer: ABE

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

NEW QUESTION 22
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.

Which two actions does FortiGate take on internet traffic sourced from the subscribers? (Choose two.)

A. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.
B. FortiGate allocates port blocks on a first-come, first-served basis.
C. FortiGate generates a system event log for every port block allocation made per user.
D. FortiGate allocates 128 port blocks per user.

Answer: BC

Explanation:
FortiGate Security 7.2 Study Guide (p.109): "FortiGate allocates port blocks on a first-come, first-served basis." "For logging purposes, when FortiGate allocates a port block to a host, it generates a system event log to inform the administrator."

NEW QUESTION 25
Refer to the exhibit.

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 30
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)

A. FortiCache
B. FortiSIEM
C. FortiAnalyzer
D. FortiSandbox
E. FortiCloud

Answer: BCE

NEW QUESTION 32
What are two features of collector agent advanced mode? (Choose two.)

A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
B. In advanced mode, security profiles can be applied only to user groups, not individual users.
C. Advanced mode uses the Windows convention—NetBios: Domain\Username.
D. Advanced mode supports nested or inherited groups.

Answer: AD

Explanation:
* A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
This is true because advanced mode allows FortiGate to query the LDAP server directly for user information and group membership, without relying on the collector agent. This enables FortiGate to apply security policies based on LDAP group filters, which can be configured on FortiGate1
* D. Advanced mode supports nested or inherited groups.
This is true because advanced mode can handle complex group structures, such as nested groups or inherited groups, where a user belongs to a group that is a member of another group. This allows FortiGate to apply security policies based on the effective group membership of a user, not just the direct group membership1
FortiGate Infrastructure 7.2 Study Guide (p.146): "Also, advanced mode supports nested or inherited groups; that is, users can be members of subgroups that belong to monitored parent groups." "In advanced mode, you can configure FortiGate as an LDAP client and configure the group filters on FortiGate. You can also configure group filters on the collector agent."

NEW QUESTION 35
An administrator needs to configure VPN user access for multiple sites using the same soft FortiToken. Each site has a FortiGate VPN gateway. What must an administrator do to achieve this objective?

A. The administrator can register the same FortiToken on more than one FortiGate.
B. The administrator must use a FortiAuthenticator device
C. The administrator can use a third-party radius OTP server.
D. The administrator must use the user self-registration server.

Answer: B

NEW QUESTION 39
Refer to the exhibits.
The exhibits show the firewall policies and the objects used in the firewall policies.
The administrator is using the Policy Lookup feature and has entered the search criteria shown in the exhibit.

Exhibit A | Exhibit B

Address Object

Name	Details
IP Range/Subnet 10	
LOCAL_CLIENT	10.0.1.10/32
all	0.0.0.0
FQDN 6	
facebook.com	facebook.com

Internet Service Object

Name	Direction	Number of Entries
Predefined Internet Services 1.635		
Facebook-Web	Destination	26.578

IP	Port	Protocol	Status
1.9.91.17 - 1.9.91.18	80	TCP	Enabled
	443		
	8443		
1.9.91.17 - 1.9.91.18	443	UDP	Enabled
1.9.91.30	443	UDP	Enabled

Firewall Policies

ID	From	To	Source	Destination	Shedule	Service	Action	NAT
3	port3	port1	LOCAL_CLIENT	facebook.com	always	ULL_UDP	ACCEPT	Enabled
1	port1	port3	facebook.com	LOCAL_CLIENT	always	ULL_UDP	ACCEPT	Enabled
4	port4	port1	LOCAL_CLIENT	all	always	HTTP DNS HTTPS	ACCEPT	Enabled
5	port3	port1	LOCAL_CLIENT	Facebook-Web	always	Internet Service	ACCEPT	Enabled
2	port3	port1	all	all	always	ALL	ACCEPT	Enabled

Exhibit A | Exhibit B

Policy Lookup

Incoming Interface	port3 ▼
IP Version	IPv4 ▼
Protocol	TCP ▼
Source	10.0.1.10
Source Port	Optional (1-65535) ↕
Destination	facebook.com
Destination Port	443 ↕

Search   Close

Which policy will be highlighted, based on the input criteria?

A. Policy with ID 4.
B. Policy with ID 5.
C. Policies with ID 2 and 3.
D. Policy with ID 4.

Answer: B

NEW QUESTION 41
Which statement describes a characteristic of automation stitches?

A. They can have one or more triggers.
B. They can be run only on devices in the Security Fabric.
C. They can run multiple actions simultaneously.

D. They can be created on any device in the fabric.

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/351998/creating-automation-stitches

NEW QUESTION 45
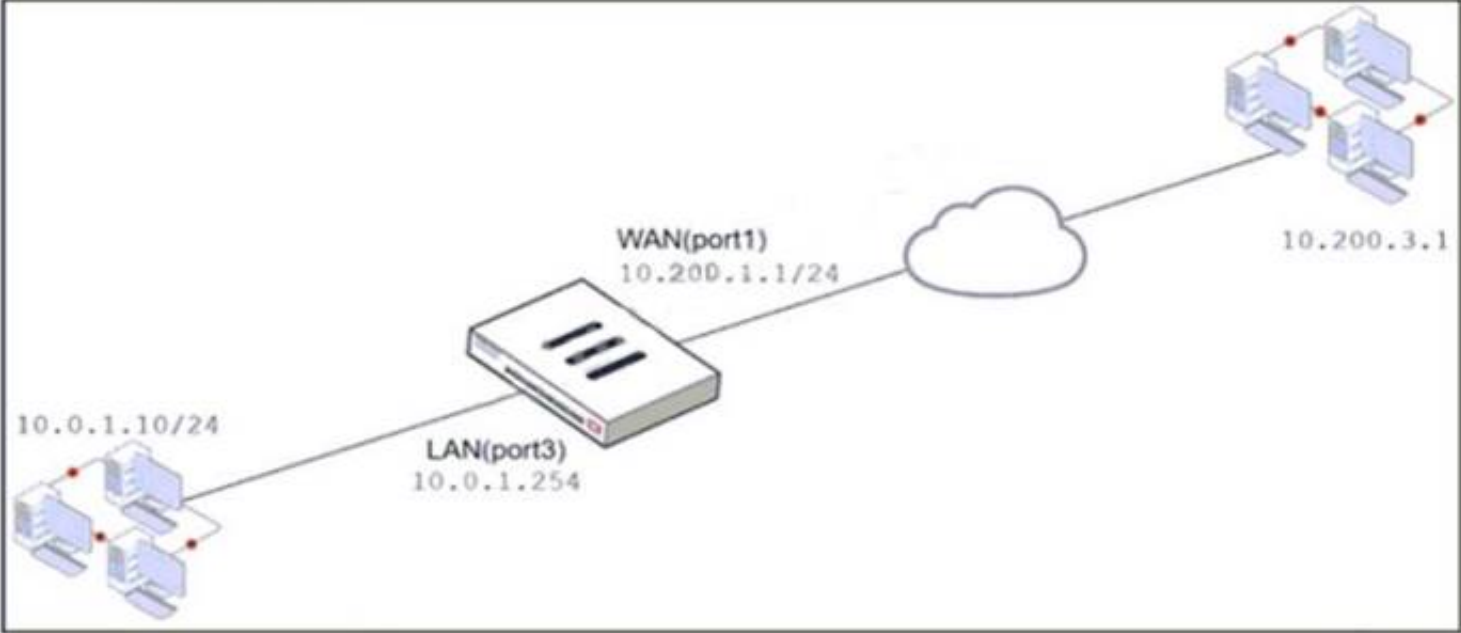Examine the exhibit, which contains a virtual IP and firewall policy configuration.

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. 10/24?

A. 10.200. 1. 10
B. Any available IP address in the WAN (port1) subnet 10.200. 1.0/24 66 of 108
C. 10.200. 1. 1
D. 10.0. 1.254

Answer: A

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs.

NEW QUESTION 46
A team manager has decided that, while some members of the team need access to a particular website, the majority of the team does not Which configuration option is the most effective way to support this request?

A. Implement a web filter category override for the specified website
B. Implement a DNS filter for the specified website.
C. Implement web filter quotas for the specified website
D. Implement web filter authentication for the specified website.

Answer: D

NEW QUESTION 50
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 53
Refer to the exhibit.

```
# diagnose test application ipsmonitor
1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command.
Which statement is correct If option 5 was used with the IPS diagnostic command and the outcome was a decrease in the CPU usage?

A. The IPS engine was inspecting high volume of traffic.
B. The IPS engine was unable to prevent an intrusion attack .
C. The IPS engine was blocking all traffic.
D. The IPS engine will continue to run in a normal state.

Answer: A

Explanation:
fortinet-fortigate-security-study-guide-for-fortios-72 page 417 If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

NEW QUESTION 57
Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

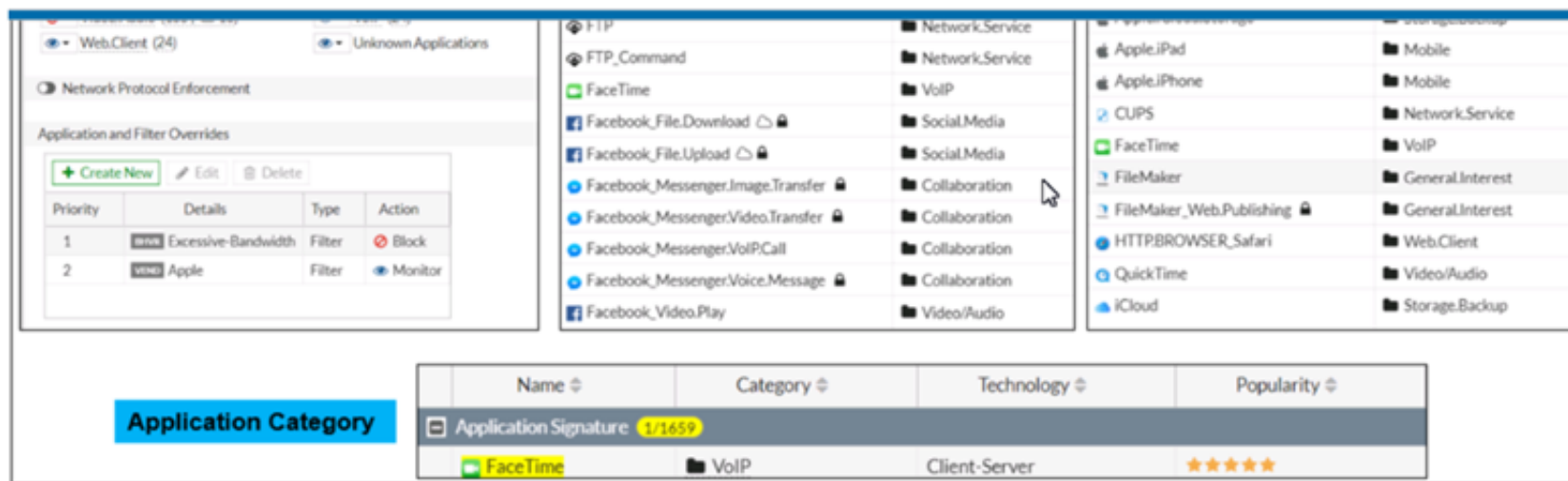A. FortiGuard web filter cache
B. FortiGate hostname
C. NTP
D. DNS

Answer: CD

Explanation:
In the 7.2 Infrastructure Guide (page 306) the list of configuration settings that are NOT synchronized includes both 'FortiGate host name' and 'Cache'

NEW QUESTION 60
Refer to the exhibit to view the application control profile.

Based on the configuration, what will happen to Apple FaceTime?

A. Apple FaceTime will be blocked, based on the Excessive-Bandwidth filter configuration
B. Apple FaceTime will be allowed, based on the Apple filter configuration.
C. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
D. Apple FaceTime will be allowed, based on the Categories configuration.

Answer: A

NEW QUESTION 65
FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy. Which two other security profiles can you apply to the security policy? (Choose two.)
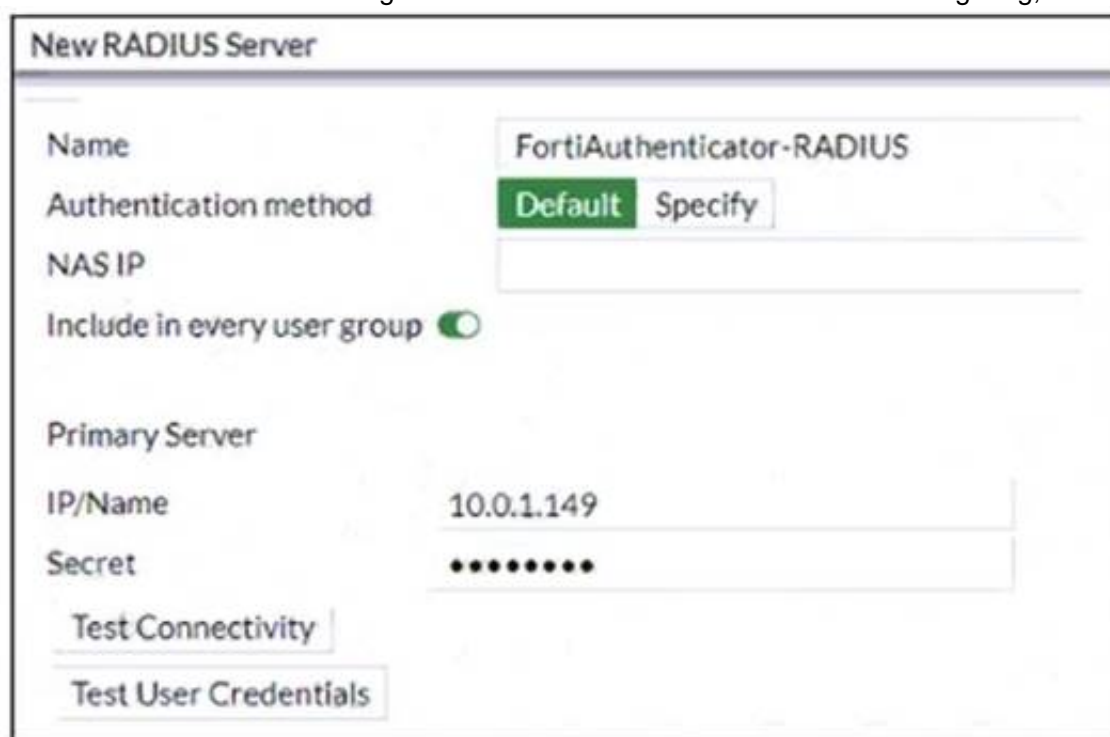
A. Antivirus scanning
B. File filter
C. DNS filter
D. Intrusion prevention

Answer: AD

NEW QUESTION 66
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.

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 71
An administrator wants to configure timeouts for users. Regardless of the userTMs behavior, the timer should start as soon as the user authenticates and expire after the configured value.
Which timeout option should be configured on FortiGate?

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

Answer: E

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-TipExplanation:-of-auth-timeout-types-for-Firewall/ta-p/

NEW QUESTION 73
Refer to the exhibit.
The exhibit shows a diagram of a FortiGate device connected to the network, the firewall policy and VIP configuration on the FortiGate device, and the routing table on the ISP router.
When the administrator tries to access the web server public address (203.0.113.2) from the internet, the connection times out. At the same time, the administrator runs a sniffer on FortiGate to capture incoming web traffic to the server and does not see any output.
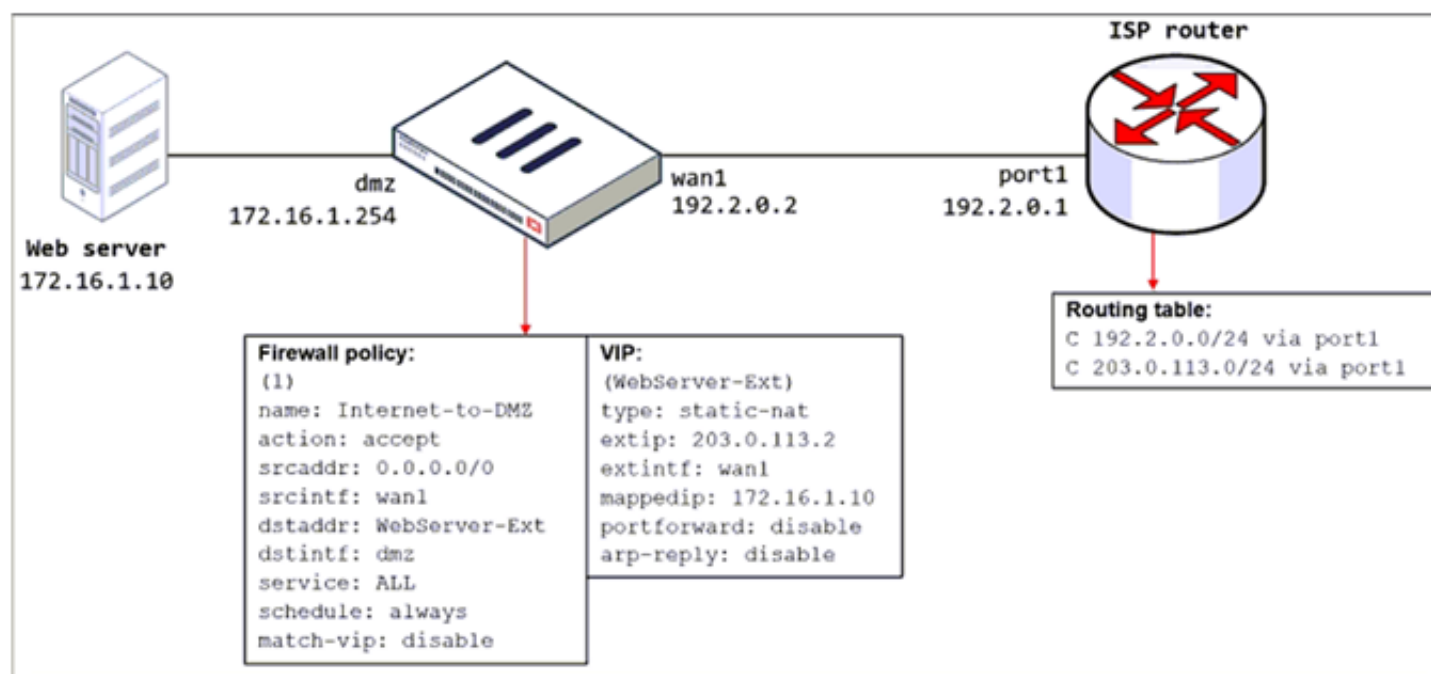
Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

A. Configure a loopback interface with address 203.0.113.2/32.
B. In the VIP configuration, enable arp-reply.
C. Enable port forwarding on the server to map the external service port to the internal service port.
D. In the firewall policy configuration, enable match-vip.

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.115): "Enabling ARP reply is usually not required in most networks because the routing tables on the adjacent devices contain the correct next hop information, so the networks are reachable. However, sometimes the routing configuration is not fully correct, and having ARP reply enabled can solve the issue for you. For this reason, it's a best practice to keep ARP reply enabled."

NEW QUESTION 74
Refer to the exhibit showing a debug flow output.

What two conclusions can you make from the debug flow output? (Choose two.)

A. The debug flow is for ICMP traffic.
B. The default route is required to receive a reply.
C. Anew traffic session was created.
D. A firewall policy allowed the connection.

Answer: AC

Explanation:
The debug flow output shows the result of a diagnose command that captures the traffic flow between the source and destination IP addresses1. The debug flow output reveals the following information about the traffic flow1:

 The protocol is 1, which means that the traffic uses ICMP protocol2. ICMP is a protocol that is used to send error messages and test connectivity between devices2.

 The session state is 0, which means that a new traffic session was created3. A session is a data structure that stores information about a connection between two devices3.

 The policy ID is 1, which means that the traffic matched the firewall policy with ID 14. A firewall policy is a rule that defines how FortiGate processes traffic based on the source, destination, service, and action parameters4.

≫ The action is 0, which means that the traffic was allowed by the firewall policy. An action is a parameter that specifies what FortiGate does with the traffic that matches a firewall policy.

Therefore, two conclusions that can be made from the debug flow output are:

≫ The debug flow is for ICMP traffic.

≫ A new traffic session was created.

NEW QUESTION 77
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: CD

NEW QUESTION 78
When configuring a firewall virtual wire pair policy, which following statement is true?

A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
B. Only a single virtual wire pair can be included in each policy.
C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
D. Exactly two virtual wire pairs need to be included in each policy.

Answer: A

NEW QUESTION 79
Refer to the exhibit.
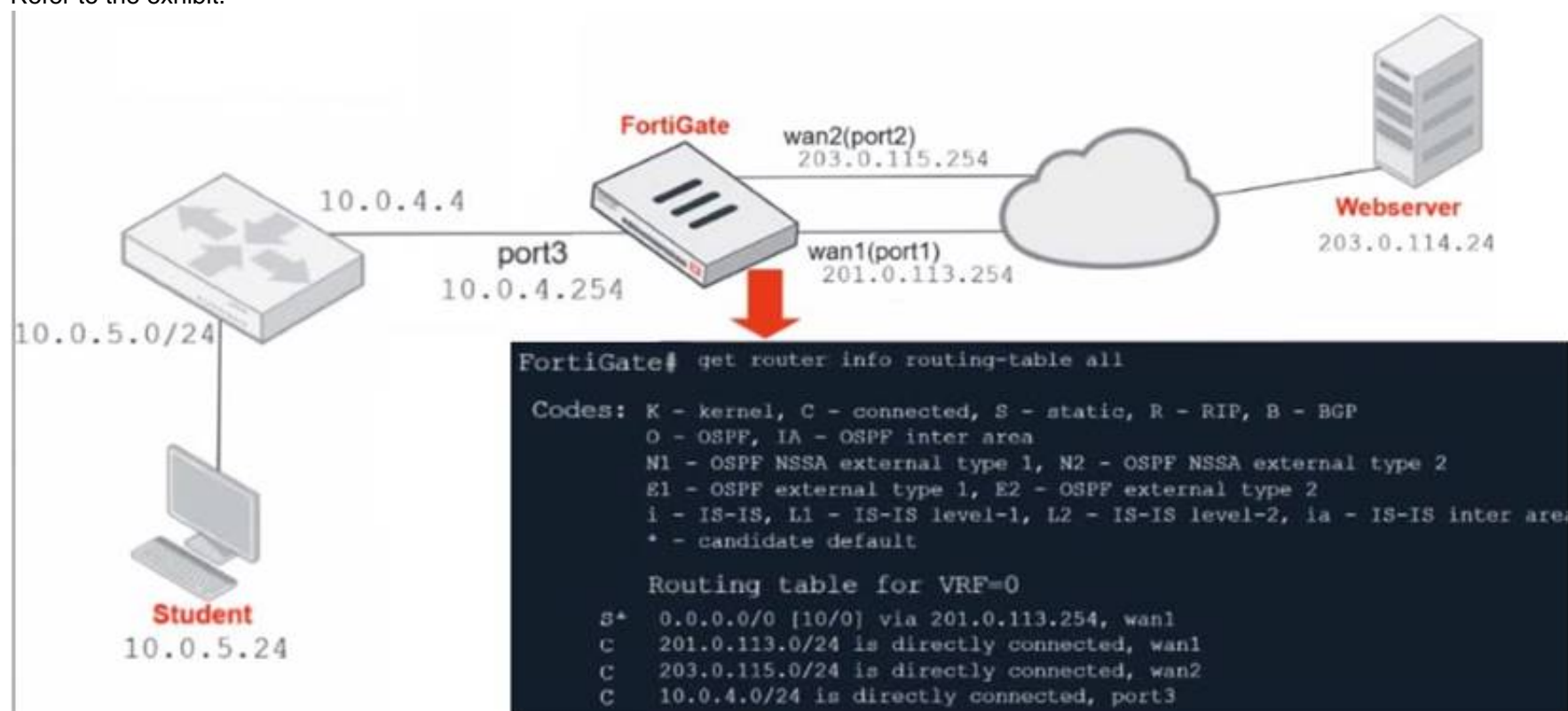
Which contains a network diagram and routing table output. The Student is unable to access Webserver.
What is the cause of the problem and what is the solution for the problem?

A. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
B. The first reply packet for Student failed the RPF check.This issue can be resolved by adding a static route to 10.0.4.0/24 through wan1.
C. The first reply packet for Student failed the RPF check .This issue can be resolved by adding a static route to 203.0. 114.24/32 through port3.
D. The first packet sent from Student failed the RPF check.This issue can be resolved by adding a static route to 203.0. 114.24/32 through port3.

Answer: D

NEW QUESTION 82
Refer to the exhibit showing a debug flow output.

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: AC

NEW QUESTION 85
......

Relate Links

100% Pass Your NSE4_FGT-7.0 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-7.0-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/