Fortinet

Exam Questions NSE4_FGT-7.2

Fortinet NSE 4 - FortiOS 7.2

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
Refer to the exhibits.
Exhibit A shows a topology for a FortiGate HA cluster that performs proxy-based inspection on traffic. Exhibit B shows the HA configuration and the partial output of the get system ha status command.
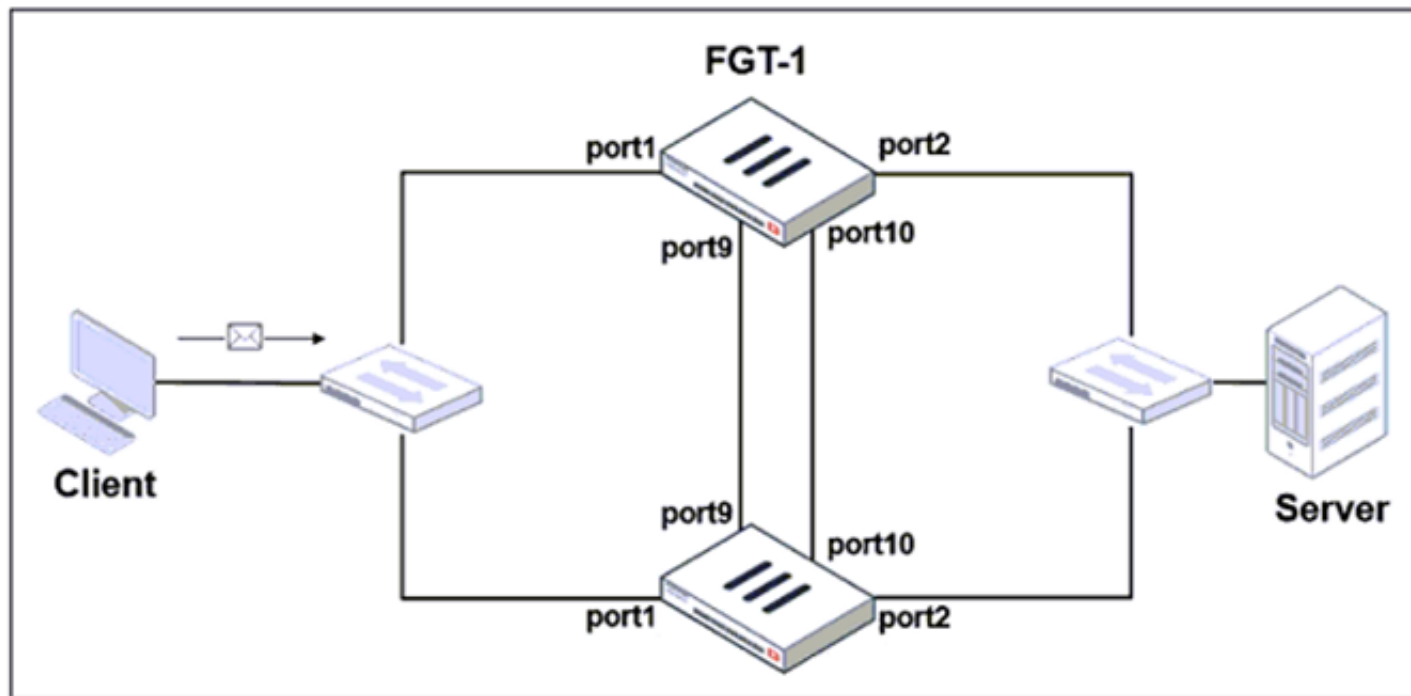
Exhibit A | Exhibit B

FGT-1

port1 port2
port9 port10

Client

port9 port10
port1 port2

Server

Exhibit A | **Exhibit B**

```
        set group-id 3
        set group-name "NSE"
        set mode a-a
        set password *
        set hbdev "port9" 50 "port10" 50
        set session-pickup enable
        set override disable
        set monitor port3
end

# get system ha status
...
Primary     : FGT-2, FGVM010000065036, HA cluster index = 1
Secondary   : FGT-1, FGVM010000064692, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000065036, HA operating index = 1
Secondary: FGVM010000064692, HA operating index = 0
```

Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)

A. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
B. The traffic sourced from the client and destined to the server is sent to FGT-1.
C. The cluster can load balance ICMP connections to the secondary.
D. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.

Answer: AD

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.317 & p.320): "To forward traffic correctly, a FortiGate HA solution uses virtual MAC addresses." "The primary forwards the SYN packet to the selected secondary. (...) This is also known as MAC address rewrite. In addition, the primary encapsulates the packet in an Ethernet frame type 0x8891. The encapsulation is done only for the first packet of a load balanced session. The encapsulated packet includes the original packet plus session information that the secondary requires to process the traffic."

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
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. 168.0.0/24
C. 192. 168.2.0/24
D. 192. 168.3.0/24

Answer: C

Explanation:
For an IPsec VPN between site A and site B, the administrator has configured the local quick mode selector for site A as 192.168.1.0/24 and the remote quick mode selector as 192.168.2.0/24. This means that the VPN will allow traffic to and from the 192.168.1.0/24 subnet at site A to reach the 192.168.2.0/24 subnet at site B.
To complete the configuration, the administrator must configure the local quick mode selector for site B. To do this, the administrator must use the same subnet as the remote quick mode selector for site A, which is 192.168.2.0/24. This will allow traffic to and from the 192.168.2.0/24 subnet at site B to reach the 192.168.1.0/24 subnet at site A.
Therefore, the administrator must configure the local quick mode selector for site B as 192.168.2.0/24.

NEW QUESTION 4
Refer to the exhibit.
The exhibit shows the FortiGuard Category Based Filter section of a corporate web filter profile.
An administrator must block access to download.com, which belongs to the Freeware and Software Downloads category. The administrator must also allow other websites in the same category.
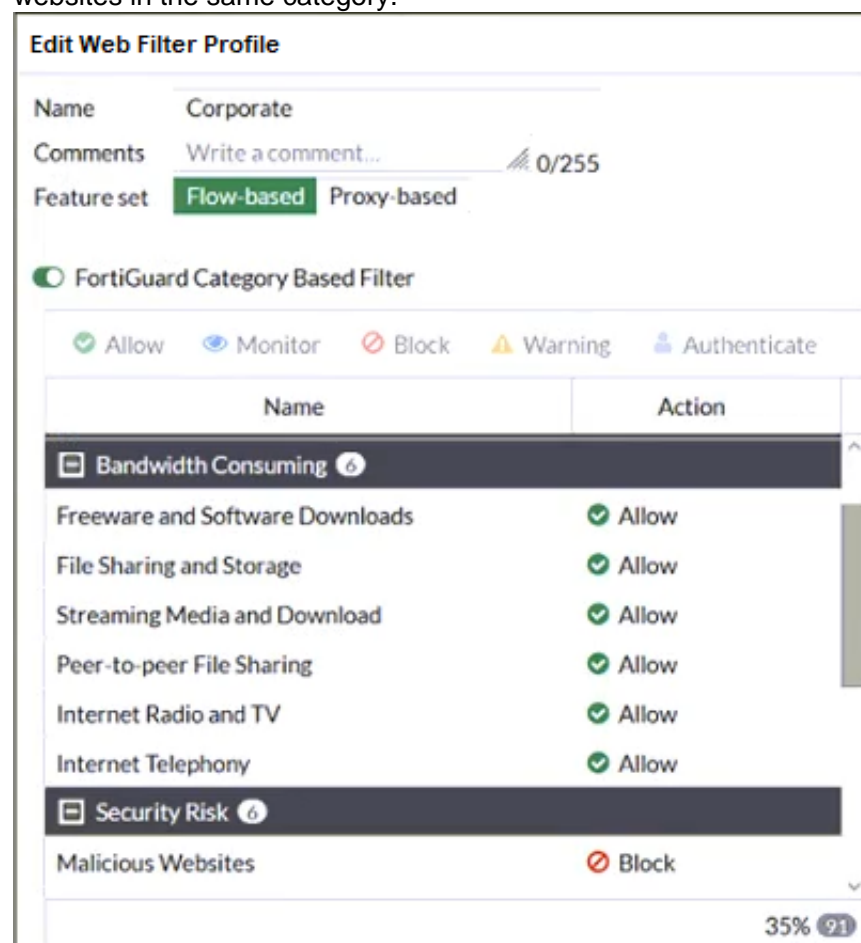
What are two solutions for satisfying the requirement? (Choose two.)

A. Configure a separate firewall policy with action Deny and an FQDN address object for *.download.com as destination address.
B. Configure a web override rating for download.com and select Malicious Websites as the subcategory.
C. Set the Freeware and Software Downloads category Action to Warning.
D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.

Answer: BD

Explanation:
FortiGate Security 7.2 Study Guide (p.268-269): "If you want to make an exception, for example, rather than unblock access to a potentially unwanted category, change the website to an allowed category. You can also do the reverse. You can block a website that belongs to an allowed category." "Static URL filtering is another web filter feature. Configured URLs in the URL filter are checked against the visited websites. If a match is found, the configured action is taken. URL filtering has the same patterns as static domain filtering: simple, regular expressions, and wildcard."
* B. Configure a web override rating for download.com and select Malicious Websites as the subcategory. This is true because a web override rating is a feature that allows the administrator to change the FortiGuard category of a specific website or domain, and apply a different action to it based on the web filter profile. By configuring a web override rating for download.com and selecting Malicious Websites as the subcategory, the administrator can block access to download.com, which belongs to the Freeware and Software Downloads category by default, without affecting other websites in the same category. The Malicious Websites category has the action Block in the web filter profile shown in the exhibit.
* D. Configure a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively.
This is true because a static URL filter entry is a feature that allows the administrator to define custom rules for filtering specific URLs or domains, and apply an action to them based on the web filter profile. By configuring a static URL filter entry for download.com with Type and Action set to Wildcard and Block, respectively, the administrator can block access to download.com and any subdomains or paths under it, without affecting other websites in the Freeware and

Software Downloads category. The static URL filter entries have higher priority than the FortiGuard category based filter entries in the web filter profile.

NEW QUESTION 5
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 NetSession Enum function is used to track user logouts.

Answer: D

Explanation:
FortiGate_Infrastructure_7.0 page 270: "NetAPI: polls temporary sessions created on the DC when a user logs in or logs out and calls the NetSessionEnum function in Windows."

NEW QUESTION 6
An employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent SSL VPN negotiation failure?

A. idle-timeout
B. login-timeout
C. udp-idle-timer
D. session-ttl

Answer: B

Explanation:
FortiGate Infrastructure 7.2 Study Guide (p.222):
"When connected to SSL VPN over high latency connections, FortiGate can time out the client before the client can finish the negotiation process, such as DNS lookup and time to enter a token. Two new CLI commands under config vpn ssl settings have been added to address this. The first command allows you to set up the login timeout, replacing the previous hard timeout value. The second command allows you to set up the maximum DTLS hello timeout for SSL VPN connections."

NEW QUESTION 7
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 8
Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

A. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
B. The client FortiGate requires a manually added route to remote subnets.
C. The client FortiGate uses the SSL VPN tunnel interface type to connect SSL VPN.
D. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.

Answer: CD

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.9/administration-guide/508779/fortigate-as-ssl-vpn-client
To establish an SSL VPN connection between two FortiGate devices, the following two settings are required:
The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate will use a CA (Certificate Authority) certificate to verify the client FortiGate certificate, ensuring that the client device is trusted and allowed to establish an SSL VPN connection.
The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: The client FortiGate must have an SSL VPN tunnel interface type configured in order to establish an SSL VPN connection. This interface type will be used to connect to the server FortiGate over the SSL VPN.

NEW QUESTION 9
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: B

Explanation:
Strict Reverse Path Forwarding (RPF) is a security feature that is used to detect and prevent IP spoofing attacks on a network. It works by checking the routing information for incoming packets to ensure that they are coming from the source address that is indicated in the packet's header. In strict RPF mode, the firewall will check the best route back to the source of the incoming packet using the incoming interface. If the packet's source address does not match the route back to the source, the packet is dropped. This helps to prevent attackers from spoofing their IP address and attempting to access the network.
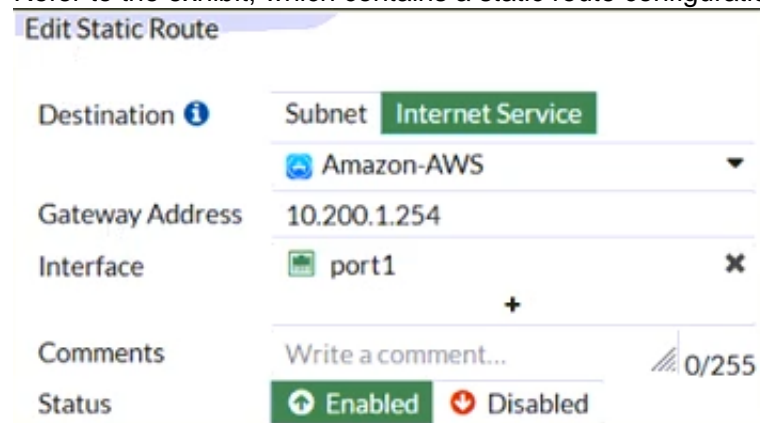
NEW QUESTION 10
An administrator does not want to report the logon events of service accounts to FortiGate. What setting on the collector agent is required to achieve this?

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

Answer: D

NEW QUESTION 10
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 14
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 17
Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)

A. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
B. Extended authentication (XAuth) to request the remote peer to provide a username and password
C. No certificate is required on the remote peer when you set the certificate signature as the authentication method
D. Pre-shared key and certificate signature as authentication methods

Answer: BD

Explanation:
* B. Extended authentication (XAuth) to request the remote peer to provide a username and password
This is true because extended authentication (XAuth) is a feature that allows FortiGate to request the remote peer to provide a username and password during the IPsec IKEv1 authentication process. XAuth is an extension of the IKEv1 protocol that adds an additional authentication step after the main mode or aggressive mode exchange. XAuth can be used with either pre-shared key or certificate signature as the primary authentication method, and it can provide stronger security and granular access control for IPsec VPNs12
* D. Pre-shared key and certificate signature as authentication methods
This is true because pre-shared key and certificate signature are two authentication methods that are supported by FortiGate for IPsec IKEv1 VPNs. Pre-shared key is a method where both peers share a secret key that is used to authenticate each other during the IKEv1 exchange. Certificate signature is a method where both peers have digital certificates that are used to verify each other's identity and public key during the IKEv1 exchange. Both methods can be combined with XAuth for additional authentication

NEW QUESTION 19
Which three statements explain a flow-based antivirus profile? (Choose three.)

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

Answer: ADE

NEW QUESTION 21
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 23
Which of the following SD-WAN load balancing method use interface weight value to distribute traffic? (Choose two.)

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

Answer: CD

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

NEW QUESTION 27
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 31
Refer to the exhibits.
Exhibit A shows the application sensor configuration. Exhibit B shows the Excessive-Bandwidth and Apple filter details.

Exhibit A | **Exhibit B**

Edit Application Sensor

Categories

▾ All Categories

✅ ▾ Business (179, ☁ 6)		✅ ▾ Cloud.IT (31)	
✅ ▾ Collaboration (293, ☁ 6)		✅ ▾ Email (87, ☁ 12)	
⊘ ▾ Game (124)		✅ ▾ General.Interest (241, ☁ 9)	
👁 ▾ Mobile (3)		✅ ▾ Network.Service (332)	
⊘ ▾ P2P (85)		⊘ ▾ Proxy (106)	
👁 ▾ Remote.Access (91)		⊘ ▾ Social.Media (150, ☁ 31)	
✅ ▾ Storage.Backup (296, ☁ 16)		✅ ▾ Update (48)	
⊘ ▾ Video/Audio (206, ☁ 13)		👁 ▾ VoIP (31)	
👁 ▾ Web.Client (18)		👁 ▾ Unknown Applications	

◯ Network Protocol Enforcement

Application and Filter Overrides

➕ Create New   ✏ Edit   🗑 Delete

Priority	Details	Type	Action
1	BHVR Excessive-Bandwidth	Filter	⊘ Block
2	VEND Apple	Filter	👁 Monitor

Exhibit A | **Exhibit B**

Edit Override

Type   Application **Filter**
Action 🚫 Block ▾
Filter   BHVR Excessive-Bandwidth   ✖
                          ✚

[FaceTime   ✖ 🔍]

Name ⇕	Category ⇕	Technology ⇕
⊟ Application Signature 1/1262		
🎥 FaceTime	📁 VoIP	Client-Server

Edit Override

Type   Application **Filter**
Action 👁 Monitor ▾
Filter   VEND Apple   ✖
                          ✚

[FaceTime   ✖ 🔍]

Name ⇕	Category ⇕	Technology ⇕
⊟ Application Signature 1/33		
🎥 FaceTime	📁 VoIP	Client-Server

Based on the configuration, what will happen to Apple FaceTime if there are only a few calls originating or incoming?

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

Answer: B

Explanation:
FortiGate Security 7.2 Study Guide (p.310): "Then, FortiGate scans packets for matches, in this order, for the application control profile: 1. Application and filter overrides: If you have configured any application overrides or filter overrides, the application control profile considers those first. It looks for a matching override starting at the top of the list, like firewall policies. 2. Categories: Finally, the application control profile applies the action that you've configured for applications in your selected categories."

NEW QUESTION 34
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: BD

NEW QUESTION 38
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 42
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

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

Answer: A

NEW QUESTION 43
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 46
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: B

Explanation:
Dialup user is used when the remote peer's IP address is unknown. The remote peer whose IP address is unknown acts as the dialup clien and this is often the case for branch offices and mobile VPN clients that use dynamic IP address and no dynamic DNS

NEW QUESTION 50
On FortiGate, which type of logs record information about traffic directly to and from the FortiGate management IP addresses?

A. System event logs
B. Forward traffic logs
C. Local traffic logs
D. Security logs

Answer: C

NEW QUESTION 53
Refer to the exhibit.

The exhibit shows the IPS sensor configuration.
If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

A. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 56
An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
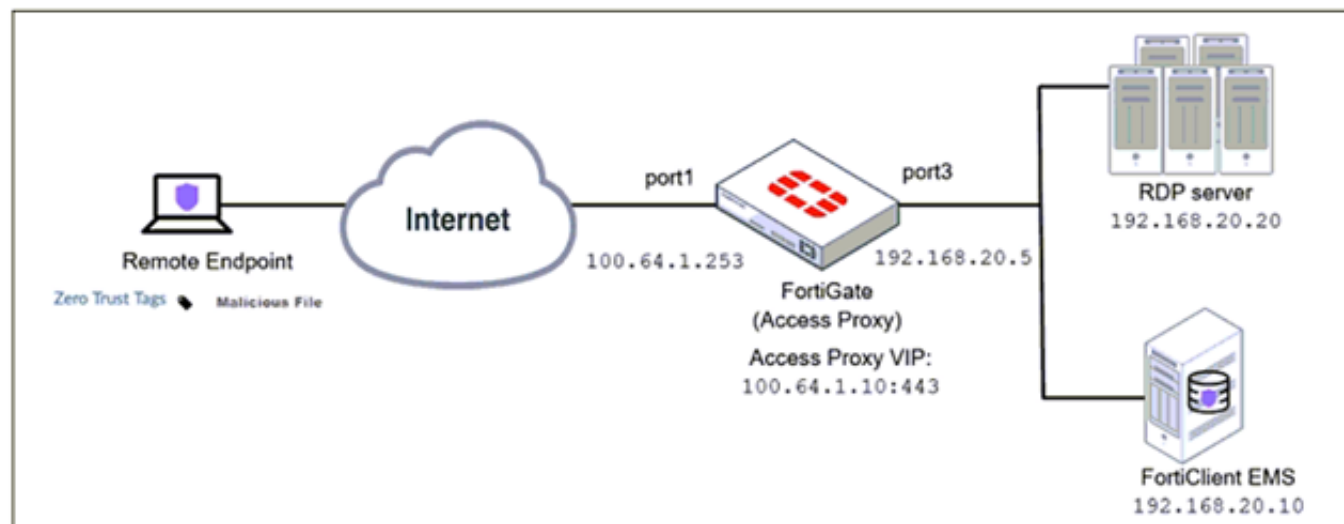Which DPD mode on FortiGate will meet the above requirement?

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

Answer: D

NEW QUESTION 57
Refer to the exhibit.

Based on the ZTNA tag, the security posture of the remote endpoint has changed. What will happen to endpoint active ZTNA sessions?

A. They will be re-evaluated to match the endpoint policy.
B. They will be re-evaluated to match the firewall policy.
C. They will be re-evaluated to match the ZTNA policy.
D. They will be re-evaluated to match the security policy.

Answer: C

Explanation:
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-zt FortiGate Infrastructure 7.2 Study Guide (p.182):
"Endpoint posture changes trigger active ZTNA proxy
sessions to be re-verified and terminated if the endpoint is no longer compliant with the ZTNA policy."

NEW QUESTION 59
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 62
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. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
B. Enable Dead Peer Detection.
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Answer: BC

Explanation:
Study Guide – IPsec VPN – IPsec configuration – Phase 1 Network.
When Dead Peer Detection (DPD) is enabled, DPD probes are sent to detect a failed tunnel and bring it down before its IPsec SAs expire. This failure detection mechanism is very useful when you have redundant paths to the same destination, and you want to failover to a backup connection when the primary connection fails to keep the connectivity between the sites up.
There are three DPD modes. On demand is the default mode. Study Guide – IPsec VPN – Redundant VPNs.
Add one phase 1 configuration for each tunnel. DPD should be enabled on both ends. Add at least one phase 2 definition for each phase 1.
Add one static route for each path. Use distance or priority to select primary routes over backup routes (routes for the primary VPN must have a lower distance or lower priority than the backup). Alternatively, use dynamic routing.
Configure FW policies for each IPsec interface.

NEW QUESTION 65
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

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

Answer: A

NEW QUESTION 67
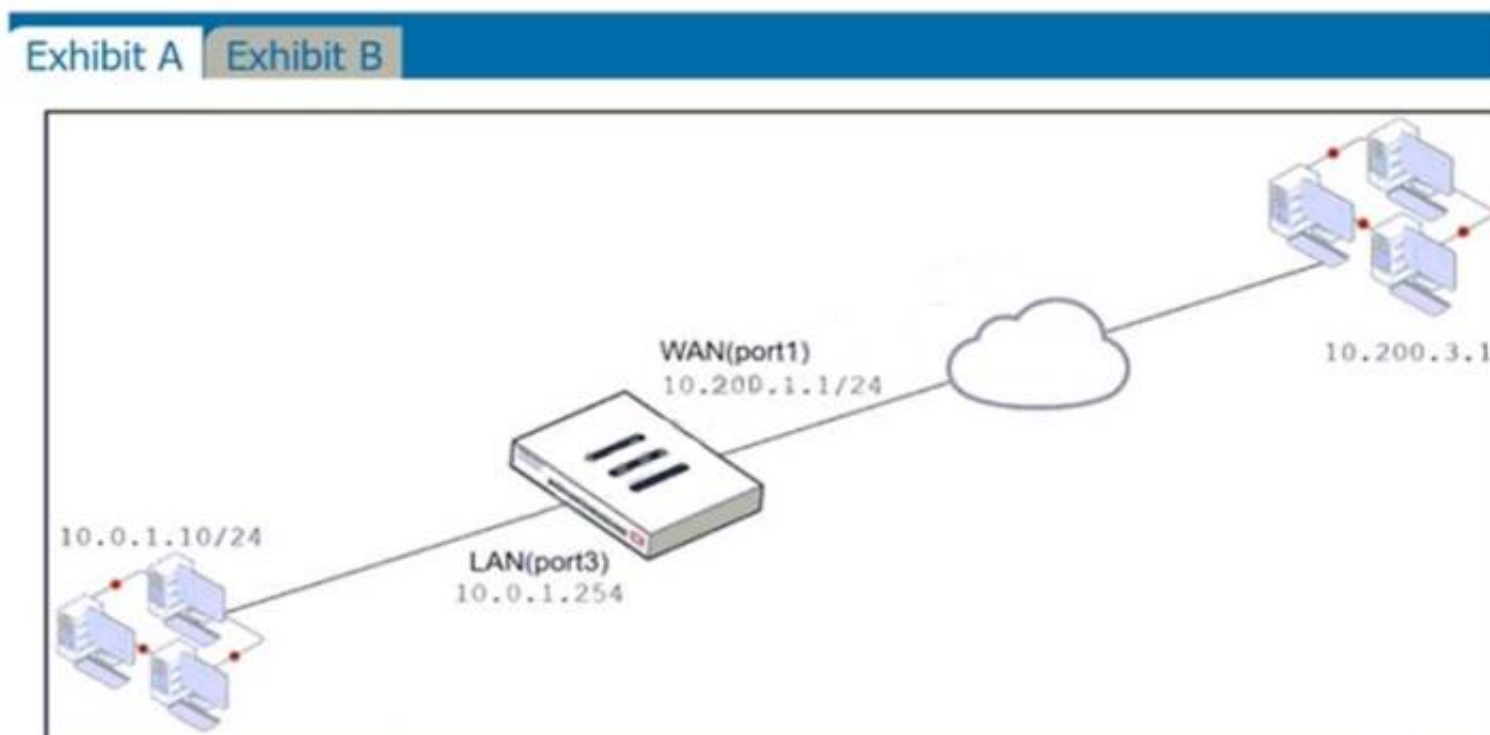Examine the exhibit, which contains a virtual IP and firewall policy configuration.

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 ❶	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 ❶	10443
Map to IPv4 port	443

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 68
What is the effect of enabling auto-negotiate on the phase 2 configuration of an IPsec tunnel?

A. FortiGate automatically negotiates different local and remote addresses with the remote peer.
B. FortiGate automatically negotiates a new security association after the existing security association expires.
C. FortiGate automatically negotiates different encryption and authentication algorithms with the remote peer.
D. FortiGate automatically brings up the IPsec tunnel and keeps it up, regardless of activity on the IPsec tunnel.

Answer: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=12069
FortiGate Infrastructure 7.2 Study Guide (p.264): "...then FortiGate might drop interesting traffic because of the absence of active SAs. To prevent this, you can enable Auto-negotiate. When you do this, FortiGate not only negotiates new SAs before the current SAs expire, but it also starts using the new SAs right away."
"Another benefit of enabling Auto-negotiate is that the tunnel comes up and stays up automatically, even when there is no interesting traffic. When you enable Autokey Keep Alive and keep Auto-negotiate disabled, the tunnel does not come up automatically unless there is interesting traffic. However, after the tunnel is up, it stays that way because FortiGate periodically sends keep alive packets over the tunnel. Note that when you enable Auto-negotiate, Autokey Keep Alive is implicitly enabled."

NEW QUESTION 70
FortiGate is operating in NAT mode and is configured with two virtual LAN (VLAN) subinterfaces added to the same physical interface.
In this scenario, which statement about VLAN IDs is true?

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

Answer: CD

NEW QUESTION 74
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 78
Refer to the exhibit.
An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.

New RADIUS Server

Name	FortiAuthenticator-RADIUS
Authentication method	**Default** Specify
NAS IP	
Include in every user group	●

Primary Server

IP/Name	10.0.1.149
Secret	••••••••

Test Connectivity

Test User Credentials

What is the impact of using the Include in every user group option in a RADIUS configuration?

A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Answer: A

NEW QUESTION 83
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.
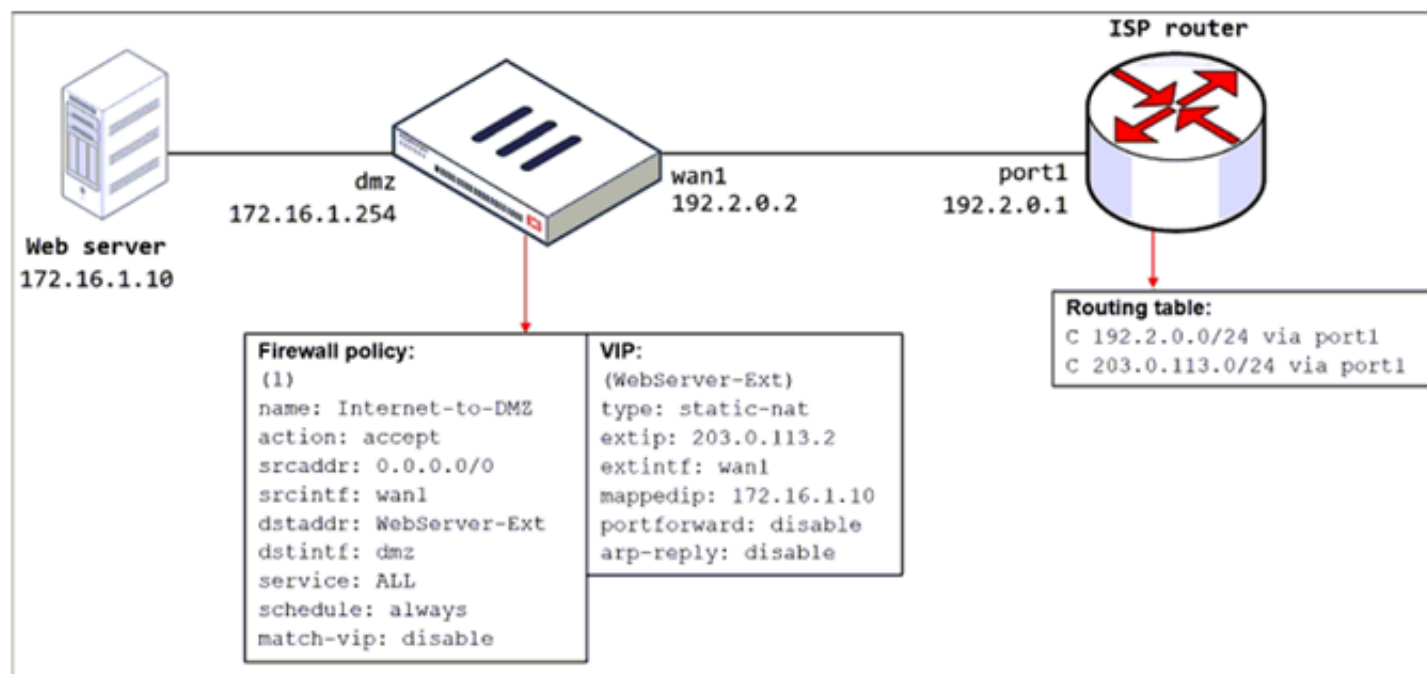
Based on the information shown in the exhibit, what configuration change must the administrator make to fix the connectivity issue?

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 88
Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

A. Subject Key Identifier value
B. SMMIE Capabilities value
C. Subject value
D. Subject Alternative Name value

Answer: A

NEW QUESTION 92
Which of statement is true about SSL VPN web mode?

A. The tunnel is up while the client is connected.
B. It supports a limited number of protocols.
C. The external network application sends data through the VPN.
D. It assigns a virtual IP address to the client.

Answer: B

Explanation:
FortiGate_Security_6.4 page 575 - Web mode requires only a web browser, but supports a limited number of protocols.

NEW QUESTION 97
Which statement about video filtering on FortiGate is true?

A. Video filtering FortiGuard categories are based on web filter FortiGuard categories.
B. It does not require a separate FortiGuard license.
C. Full SSL inspection is not required.
D. its available only on a proxy-based firewall policy.

Answer: D

Explanation:
FortiGate Security 7.2 Study Guide (p.279): "To apply the video filter profile, proxy-based firewall polices currently allow you to enable the video filter profile. You must enable full SSL inspection on the firewall policy."
https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/860867/filtering-based-on-fortiguard-cat

NEW QUESTION 99
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 104
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 108
......

Relate Links

100% Pass Your NSE4_FGT-7.2 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-7.2-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/