Fortinet.NSE4_FGT-7.2.v2023-09-04.q73

Exam Code:	NSE4_FGT-7.2
Exam Name:	Fortinet NSE 4 - FortiOS 7.2
Certification Provider:	Fortinet
Free Question Number:	73
Version:	v2023-09-04
# of views:	3443
# of Questions views:	730
https://www.freepdfdumps.com/Fortinet.NSE4_FGT-7.2.v2023-09-04.q73.html	

NEW QUESTION: 1
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 new traffic session is created.
C. The default route is required to receive a reply.
D. A firewall policy allowed the connection.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which two statements are correct regarding FortiGate HA cluster virtual IP addresses? (Choose two.)
A. Virtual IP addresses are used to distinguish between cluster members.
B. The primary device in the cluster is always assigned IP address 169.254.0.1.
C. Heartbeat interfaces have virtual IP addresses that are manually assigned.
D. A change in the virtual IP address happens when a FortiGate device joins or leaves the cluster.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 3
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: (SHOW ANSWER)
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: 4
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. new-session
B. idle-timeout
C. auth-on-demand
D. hard-timeout
E. soft-timeout
Answer: (SHOW ANSWER)

NEW QUESTION: 5
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: (SHOW ANSWER)
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: 6
Refer to the exhibit.
Which contains a session list output. Based on the information shown in the exhibit, which statement is true?

A. Destination NAT is disabled in the firewall policy.
B. One-to-one NAT IP pool is used in the firewall policy.
C. Overload NAT IP pool is used in the firewall policy.
D. Port block allocation IP pool is used in the firewall policy.
Answer: B (LEAVE A REPLY)
Explanation
FortiGate_Security_6.4 page 155 . In one-to-one, PAT is not required.

NEW QUESTION: 7
Refer to the exhibits.
Exhibit A.
Exhibit B.
An administrator creates a new address object on the root FortiGate (Local-FortiGate) in the security fabric.
After synchronization, this object is not available on the downstream FortiGate (ISFW).
What must the administrator do to synchronize the address object?
A. Change the csf setting on Local-FortiGate (root) to set configuration-sync local.
B. Change the csf setting on ISFW (downstream) to set fabric-object-unification default.
C. Change the csf setting on Local-FortiGate (root) to set fabric-object-unification default.
D. Change the csf setting on ISFW (downstream) to set configuration-sync local.
Answer: (SHOW ANSWER)

NEW QUESTION: 8
Which three options are the remote log storage options you can configure on FortiGate? (Choose three.)
A. FortiAnalyzer
B. FortiCache
C. FortiSIEM
D. FortiSandbox
E. FortiCloud
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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 (LEAVE A REPLY)

Explanation
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/580880/posture-check-verification-for-active-ztn

NEW QUESTION: 10
Refer to the web filter raw logs.
Based on the raw logs shown in the exhibit, which statement is correct?
A. Social networking web filter category is configured with the action set to authenticate.
B. Access to the social networking web filter category was explicitly blocked to all users.
C. The name of the firewall policy is all_users_web.
D. The action on firewall policy ID 1 is set to warning.
Answer: (SHOW ANSWER)

NEW QUESTION: 11
An administrator has configured the following settings:
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.
Answer: C,D (LEAVE A REPLY)
Explanation
ses-denied-traffic
Enable/disable including denied session in the session table.
https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/20620/config-system-settings
block-session-timer Duration in seconds for blocked sessions .
integer
Minimum value: 1 Maximum value: 300
30
https://docs.fortinet.com/document/fortigate/7.0.6/cli-reference/1620/config-system-global

NEW QUESTION: 12
When configuring a firewall virtual wire pair policy, which following statement is true?
A. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
B. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
C. Exactly two virtual wire pairs need to be included in each policy.
D. Only a single virtual wire pair can be included in each policy.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
Refer to the exhibit.
The global settings on a FortiGate device must be changed to align with company security policies. What does the Administrator account need to access the FortiGate global settings?
A. Change password
B. Enable restrict access to trusted hosts
C. Enable two-factor authentication
D. Change Administrator profile
Answer: (SHOW ANSWER)

NEW QUESTION: 14
An organization's employee needs to connect to the office through a high-latency internet connection.
Which SSL VPN setting should the administrator adjust to prevent the SSL VPN negotiation failure?
A. Change the idle-timeout.
B. Change the session-ttl.
C. Change the udp idle timer.
D. Change the login timeout.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
Refer to the exhibit.
An administrator is running a sniffer command as shown in the exhibit.
Which three pieces of information are included in the sniffer output? (Choose three.)
A. IP header
B. Interface name
C. Ethernet header
D. Packet payload
E. Application header
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 16
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, what configuration change will bring phase 2 up?
A. On HQ-FortiGate, set Encryption to AES256.
B. On HQ-FortiGate, enable Diffie-Hellman Group 2.
C. On Remote-FortiGate, set Seconds to 43200.

D. On HQ-FortiGate, enable Auto-negotiate.
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Consider the topology:
Application on a Windows machine <--{SSL VPN} -->FGT--> Telnet to Linux server.
An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.
The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.
What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)
A. Set the maximum session TTL value for the TELNET service object.
B. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.
C. Create a new service object for TELNET and set the maximum session TTL.
D. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 18
What are two functions of ZTNA? (Choose two.)
A. ZTNA manages access through the client only.
B. ZTNA provides role-based access.
C. ZTNA provides a security posture check.
D. ZTNA manages access for remote users only.
Answer: (SHOW ANSWER)

NEW QUESTION: 19
Which two statements are correct about NGFW Policy-based mode? (Choose two.)

A. NGFW policy-based mode supports creating applications and web filtering categories directly in a firewall policy
B. NGFW policy-based mode does not require the use of central source NAT policy
C. NGFW policy-based mode can only be applied globally and not on individual VDOMs
D. NGFW policy-based mode policies support only flow inspection
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 20
Refer to the exhibits.
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: (SHOW ANSWER)
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.

NEW QUESTION: 21
Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)
A. Uninterruptable upgrade is enabled by default.
B. Traffic load balancing is temporally disabled while upgrading the firmware.
C. Only secondary FortiGate devices are rebooted.
D. The firmware image must be manually uploaded to each FortiGate.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 22
In which two ways can RPF checking be disabled? (Choose two)
A. Enable asymmetric routing.
B. Enable anti-replay in firewall policy.
C. Disable the RPF check at the FortiGate interface level for the source check
D. Disable strict-arc-check under system settings.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 23
Which timeout setting can be responsible for deleting SSL VPN associated sessions?
A. SSL VPN dtls-hello-timeout
B. SSL VPN idle-timeout
C. SSL VPN login-timeout
D. SSL VPN http-request-body-timeout
Answer: B (LEAVE A REPLY)

NEW QUESTION: 24
Refer to the exhibits.
The SSL VPN connection fails when a user attempts to connect to it. What should the user do to successfully connect to SSL VPN?
A. Change the Server IP address.
B. Change the SSL VPN port on the client.
C. Change the SSL VPN portal to the tunnel.
D. Change the idle-timeout.
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Why does FortiGate Keep TCP sessions in the session table for several seconds, even after both sides (client and server) have terminated the session?
A. To allow for out-of-order packets that could arrive after the FIN/ACK packets
B. To finish any inspection operations
C. To remove the NAT operation
D. To generate logs
Answer: A (LEAVE A REPLY)
Explanation
TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end. This is called a half-close. FortiGate unit implements a specific timer before removing an entry in the firewall session table.

NEW QUESTION: 26
Which statement about the policy ID number of a firewall policy is true?
A. It is required to modify a firewall policy using the CLI.
B. It represents the number of objects used in the firewall policy.
C. It defines the order in which rules are processed.
D. It changes when firewall policies are reordered.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27

Refer to the exhibit.
Based on the raw log, which two statements are correct? (Choose two.)
A. Traffic is blocked because Action is set to DENY in the firewall policy.
B. This is a security log.
C. Log severity is set to error on FortiGate.
D. Traffic belongs to the root VDOM.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 28
Refer to the exhibit.
The exhibit contains a network diagram, virtual IP, IP pool, and firewall policies configuration.
The WAN (port1) interface has the IP address 10.200. 1. 1/24.
The LAN (port3) interface has the IP address 10 .0.1.254. /24.
The first firewall policy has NAT enabled using IP Pool.
The second firewall policy is configured with a VIP as the destination address.
Which IP address will be used to source NAT the internet traffic coming from a workstation with the IP address 10.0. 1. 10?
A. 10.200. 1. 1
B. 10.200.3. 1
C. 10.200. 1. 100
D. 10.200. 1. 10
Answer: C (LEAVE A REPLY)
Explanation
Policy 1 is applied on outbound (LAN-WAN) and policy 2 is applied on inbound (WAN-LAN). question is asking SNAT for outbound traffic so policy 1 will take place and NAT overload is in effect.

NEW QUESTION: 29
Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)
A. udp-echo
B. DNS
C. ping
D. TWAMP
Answer: (SHOW ANSWER)

NEW QUESTION: 30
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: A,B,E (LEAVE A REPLY)
Explanation
https://docs.fortinet.com/document/fortigate/7.0.0/new-features/739623/dns-filter-handled-by-ips-engine-in-flow

NEW QUESTION: 31
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)
A. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.
B. ADVPN is only supported with IKEv2.
C. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
D. Tunnels are negotiated dynamically between spokes.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 32
Refer to the exhibit.
Based on the administrator profile settings, what permissions must the administrator set to run the diagnose firewall auth list CLI command on FortiGate?
A. Custom permission for Network
B. Read/Write permission for Log & Report
C. CLI diagnostics commands permission
D. Read/Write permission for Firewall
Answer: C (LEAVE A REPLY)
Explanation
https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220

NEW QUESTION: 33
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. 10.200.3.1, 10.0.1.10, and 443, respectively
B. 10.0.1.254, 10.0.1.10, and 10443, respectively
C. 10.0.1.254, 10.0.1.10, and 443, respectively
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
What is the limitation of using a URL list and application control on the same firewall policy, in NGFW policy-based mode?
A. It limits the scope of application control to scan application traffic on DNS protocol only.
B. It limits the scope of application control to scan application traffic based on application category only.
C. It limits the scope of application control to the browser-based technology category only.
D. It limits the scope of application control to scan application traffic using parent signatures only
Answer: (SHOW ANSWER)

NEW QUESTION: 35
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 have IP addresses in different subnets.
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 belong to different VDOMs.
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 36
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: (SHOW ANSWER)
Explanation
Port 1 shows the lowest latency.

NEW QUESTION: 37
Refer to the exhibit.
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 unable to prevent an intrusion attack .
B. The IPS engine was inspecting high volume of traffic.
C. The IPS engine will continue to run in a normal state.
D. The IPS engine was blocking all traffic.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
Refer to the exhibit.
The Root and To_Internet VDOMs are configured in NAT mode. The DMZ and Local VDOMs are configured in transparent mode.
The Root VDOM is the management VDOM. The To_Internet VDOM allows LAN users to access the internet. The To_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem .
With this configuration, which statement is true?
A. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.
B. A static route is required on the To_Internet VDOM to allow LAN users to access the internet.
C. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
D. Inter-VDOM links are required to allow traffic between the Local and DMZ VDOMs.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
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 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.
B. 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.
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 10.0.4.0/24 through wan1.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
Which statement regarding the firewall policy authentication timeout is true?
A. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source IP.
B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this timer has expired.
C. It is an idle timeout. The FortiGate considers a user to be "idle" if it does not see any packets coming from the user's source MAC.
D. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this timer has expired.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
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 (LEAVE A REPLY)
Explanation
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Objects/Virtual%20IPs.

NEW QUESTION: 42
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. execute traceroute
B. diagnose sniffer packet any
C. get system arp

D. execute ping
E. diagnose sys top
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 43
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 only if the filter in Application and Filter Overrides is set to Learn
C. Apple FaceTime will be allowed, based on the Apple filter configuration.
D. Apple FaceTime will be allowed, based on the Categories configuration.
Answer: (SHOW ANSWER)

NEW QUESTION: 44
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 gather a packet log for all matched traffic.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will allow attackers matching the Microsoft Windows.iSCSI.Target.DoS signature.
D. The sensor will reset all connections that match these signatures.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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: (SHOW ANSWER)
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: 46
An administrator has a requirement to keep an application session from timing out on port 80.
What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)
A. Set the session TTL on the HTTP policy to maximum

B. Create a new service object for HTTP service and set the session TTL to never
C. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
D. Set the TTL value to never under config system-ttl
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 47
Which two types of traffic are managed only by the management VDOM? (Choose two.)
A. PKI
B. FortiGuard web filter queries
C. Traffic shaping
D. DNS
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 48
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 CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
B. FortiGate does not support full SSL inspection when web filtering is enabled.
C. There are network connectivity issues.
D. The browser requires a software update.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 49
Examine this PAC file configuration.
Which of the following statements are true? (Choose two.)
A. Any web request fortinet.com is allowed to bypass the proxy.
B. Any web request to the 172.25. 120.0/24 subnet is allowed to bypass the proxy.

C. All requests not made to Fortinet.com or the 172.25. 120.0/24 subnet, have to go through altproxy.corp.com: 8060.
D. Browsers can be configured to retrieve this PAC file from the FortiGate.
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 50
What are two benefits of flow-based inspection compared to proxy-based inspection? (Choose two.)
A. FortiGate allocates two sessions per connection.
B. FortiGate adds less latency to traffic.
C. FortiGate uses fewer resources.
D. FortiGate performs a more exhaustive inspection on traffic.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 51
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.
Based on the exhibits, which two statements about the traffic passing through the cluster are true? (Choose two.)
A. For load balanced connections, the primary encapsulates TCP SYN packets before forwarding them to the secondary.
B. For non-load balanced connections, packets forwarded by the cluster to the server contain the virtual MAC address of port2 as source.
C. The cluster can load balance ICMP connections to the secondary.
D. The traffic sourced from the client and destined to the server is sent to FGT-1.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 52
Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)
A. HTTPS
B. FTM
C. FortiTelemetry
D. SSH
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 53
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: D (LEAVE A REPLY)

NEW QUESTION: 54
Which of the following conditions must be met in order for a web browser to trust a web server certificate signed by a third-party CA?
A. The web-server 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 private key of the CA certificate that signed the browser certificate must be installed on the browser.
D. The public key of the web server certificate must be installed on the browser.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
Refer to the exhibit.
The exhibit shows the output of a diagnose command.
What does the output reveal about the policy route?
A. It is an SDWAN rule in policy route.
B. It is an ISDB policy route with an SDWAN rule.
C. It is an ISDB route in policy route.
D. It is a regular policy route.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
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 (LEAVE A REPLY)

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.

NEW QUESTION: 57
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 web filter quotas for the specified website
B. Implement a web filter category override for the specified website
C. Implement web filter authentication for the specified website.
D. Implement a DNS filter for the specified website.
Answer: (SHOW ANSWER)

NEW QUESTION: 58
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: (SHOW ANSWER)

NEW QUESTION: 59
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, enable Auto-negotiate.
C. On HQ-FortiGate, enable Diffie-Hellman Group 2.
D. On HQ-FortiGate, set Encryption to AES256.
Answer: (SHOW ANSWER)

NEW QUESTION: 60
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.
Which policy will be highlighted, based on the input criteria?
A. Policies with ID 2 and 3.
B. Policy with ID 4.
C. Policy with ID 5.
D. Policy with ID 4.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
Which of the following statements about central NAT are true? (Choose two.)
A. Central NAT can be enabled or disabled from the CLI only.
B. IP tool references must be removed from existing firewall policies before enabling central NAT .
C. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.
D. Source NAT, using central NAT, requires at least one central SNAT policy.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 62
Refer to the exhibit.
Given the routing database shown in the exhibit, which two statements are correct? (Choose two.)
A. The port3 default route has the lowest metric.
B. The port3 default route has the highest distance.
C. The port1 and port2 default routes are active in the routing table.
D. There will be eight routes active in the routing table.
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 63
Which two statements ate true about the Security Fabric rating? (Choose two.)
A. It provides executive summaries of the four largest areas of security focus.
B. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
C. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.
D. Many of the security issues can be fixed immediately by clicking Apply where available.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 64
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 Enable probe packets setting is not enabled.
B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
C. The Detection Mode setting is not set to Passive.
D. The configured participants are not SD-WAN members.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 65
Which feature in the Security Fabric takes one or more actions based on event triggers?
A. Automation Stitches
B. Security Rating
C. Logical Topology
D. Fabric Connectors
Answer: A (LEAVE A REPLY)

NEW QUESTION: 66
An administrator configures FortiGuard servers as DNS servers on FortiGate using default settings.
What is true about the DNS connection to a FortiGuard server?
A. It uses DNS over HTTPS.
B. It uses DNS overTLS.
C. It uses UDP 53.
D. It uses UDP 8888.
Answer: (SHOW ANSWER)

NEW QUESTION: 67

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

A. hard-timeout

B. auth-on-demand

C. soft-timeout

D. new-session

E. Idle-timeout

Answer: A,D,E (LEAVE A REPLY)

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

NEW QUESTION: 68

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 generates a system event log for every port block allocation made per user.

B. FortiGate allocates port blocks on a first-come, first-served basis.

C. FortiGate allocates port blocks per user, based on the configured range of internal IP addresses.

D. FortiGate allocates 128 port blocks per user.

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 69

In consolidated firewall policies, IPv4 and IPv6 policies are combined in a single consolidated policy. Instead of separate policies. Which three statements are true about consolidated IPv4 and IPv6 policy configuration?

(Choose three.)

A. The IP version of the sources and destinations in a firewall policy must be different.

B. The Incoming Interface. Outgoing Interface. Schedule, and Service fields can be shared with both IPv4 and IPv6.

C. The IP version of the sources and destinations in a policy must match.

D. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.

Answer: B,C,D (LEAVE A REPLY)

NEW QUESTION: 70

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

A. AH does not provide any data integrity or encryption.

B. AH does not support perfect forward secrecy.
C. AH provides data integrity bur no encryption.
D. AH provides strong data integrity but weak encryption.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
Refer to the exhibits.
Exhibit A shows system performance output. Exhibit B shows a FortiGate configured with the default configuration of high memory usage thresholds. Based on the system performance output, which two statements are correct? (Choose two.)
A. Administrators can access FortiGate only through the console port.
B. FortiGate has entered conserve mode.
C. Administrators cannot change the configuration.
D. FortiGate will start sending all files to FortiSandbox for inspection.
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?
A. diagnose wad session list | grep hook-pre&&hook-out
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
Answer: D (LEAVE A REPLY)

NEW QUESTION: 73
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, disable Diffie-Helman group 2.
B. On Remote-FortiGate, set port2 as Interface.
C. On both FortiGate devices, set Dead Peer Detection to On Demand.
D. On HQ-FortiGate, set IKE mode to Main (ID protection).
Answer: B,D (LEAVE A REPLY)