Exam Questions NSE4_FGT-6.4

Fortinet NSE 4 - FortiOS 6.4

https://www.2passeasy.com/dumps/NSE4_FGT-6.4/

NEW QUESTION 1
Which two actions can you perform only from the root FortiGate in a Security Fabric? (Choose two.)

A. Shut down/reboot a downstream FortiGate device.
B. Disable FortiAnalyzer logging for a downstream FortiGate device.
C. Log in to a downstream FortiSwitch device.
D. Ban or unban compromised hosts.

Answer: A

NEW QUESTION 2
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: AB

NEW QUESTION 3
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. Many of the security issues can be fixed immediately by click ng Apply where available.
C. The Security Fabric rating must be run on the root FortiGate device in the Security Fabric.
D. The Security Fabric rating is a free service that comes bundled with alt FortiGate devices.

Answer: AC

NEW QUESTION 4
View the exhibit.

Which of the following statements are correct? (Choose two.)

A. This setup requires at least two firewall policies with the action set to IPsec.
B. Dead peer detection must be disabled to support this type of IPsec setup.
C. The TunnelB route is the primary route for reaching the remote sit
D. The TunnelA route is used only if the TunnelB VPN is down.
E. This is a redundant IPsec setup.

Answer: CD

NEW QUESTION 5
If the Issuer and Subject values are the same in a digital certificate, which type of entity was the certificate issued to?

A. A CRL
B. A person
C. A subordinate CA
D. A root CA

Answer: D

NEW QUESTION 6
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 192.160.1.0/24 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: B

NEW QUESTION 7
Refer to the exhibit.

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

A. port1-vlan1 and port2-vlan1 can be assigned in the same VDOM or to different VDOMs

B. port1 is a native VLAN.
C. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
D. Traffic between port2 and port2-vlan1 is allowed by default.

Answer: CD

NEW QUESTION 8
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: C

NEW QUESTION 9
Refer to the exhibit.

Which contains a PerformanceSLA configuration.
An administrator has configured a performance SLA on FortiGate. Which failed to generate any traffic. Why is FortiGate not generating any traffic for the performance SLA?

A. Participants configured are not SD-WAN members.
B. There may not be a static route to route the performance SLA traffic.
C. The Ping protocol is not supported for the public servers that are configured.
D. You need to turn on the Enable probe packets switch.

Answer: D

NEW QUESTION 10
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: A

NEW QUESTION 10
By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which two CLI commands will cause FortiGate to use an unreliable protocol to communicate with FortiGuard servers for live web filtering? (Choose two.)

A. set fortiguard anycast disable
B. set protocol udp
C. set webfilter-force-off disable
D. set webfilter-cache disable

Answer: AC

NEW QUESTION 13
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: B

NEW QUESTION 18
Which two statements are true about the FGCP protocol? (Choose two.)

A. Not used when FortiGate is in Transparent mode
B. Elects the primary FortiGate device
C. Runs only over the heartbeat links
D. Is used to discover FortiGate devices in different HA groups

Answer: CD

NEW QUESTION 19
Refer to the exhibit.

According to the certificate values shown in the exhibit, which type of entity was the certificate issued to?

A. A user
B. A root CA
C. A bridge CA
D. A subordinate

Answer: A

NEW QUESTION 23
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. FortiGate will start sending all files to FortiSandbox for inspection.
D. Administrators cannot change the configuration.

Answer: CD

NEW QUESTION 24
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 28
If theServicesfield is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

A. TheServicesfield prevents SNAT and DNAT from being combined in the same policy.
B. TheServicesfield is used when you need to bundle several VIPs into VIP groups.

C. TheServicesfield removes the requirement to create multiple VIPs for different services.
D. TheServicesfield prevents multiple sources of traffic from using multiple services to connect to a singlecomputer.

Answer: C

NEW QUESTION 30
Refer to theexhibits.

The exhibits show the SSL and authentication policy (Exhibit A) and the security policy (Exhibit B) tor Facebook.
Users are given access to the Facebook web application. They can play video content hosted on Facebook but they areunableto leavereactions on videos or other types ofposts.
Which part ofthe policy configuration must you change to resolve the issue?

A. The SSL inspection needs tobe a deep content inspection.
B. Force access to Facebook using the HTTP service.
C. Additional application signatures arerequired to add to thesecurity policy.
D. Add Facebook in the URL category in the security policy.

Answer: A

NEW QUESTION 33
When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

A. remote user's public IP address
B. The public IP address of the FortiGate device.
C. The remote user's virtual IP address.
D. The internal IP address of the FortiGate device.

Answer: D

Explanation:
Source IP seen by the remote resources is FortiGate's internal IP address and not the user's IP address

NEW QUESTION 38
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,enable Auto-negotiate.
B. On Remote-FortiGate, set Seconds to 43200.
C. On HQ-FortiGate,enable Diffie-Hellman Group 2.
D. On HQ-FortiGate, set Encryption to AES256.

Answer: D

NEW QUESTION 42
Which two settings can be separately configured per VDOM on a FortiGate device? (Choose two.)

A. System time
B. FortiGuaid update servers
C. Operating mode
D. NGFW mode

Answer: AD

NEW QUESTION 46
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: ADE

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

NEW QUESTION 47
Examine this FortiGate configuration:

How does the FortiGate handle web proxy traffic coming from the IP address 10.2.1.200 that requires authorization?

A. It always authorizes the traffic without requiring authentication.
B. It drops the traffic.
C. It authenticates the traffic using the authentication scheme SCHEME2.
D. It authenticates the traffic using the authentication scheme SCHEME1.

Answer: D

Explanation:
"What happens to traffic that requires authorization, but does not match any authentication rule? The active and passive SSO schemes to use for those cases is defined under config authentication setting"

NEW QUESTION 49
Examine the IPS sensor configuration shown in the exhibit, and then answer the question below.

An administrator has configured the WINDOWS_SERVERS IPS sensor in an attempt to determine
whether the influx of HTTPS traffic is an attack attempt or not. After applying the IPS sensor, FortiGate is still not generating any IPS logs for the HTTPS traffic.
What is a possible reason for this?

A. The IPS filter is missing the Protocol: HTTPS option.
B. The HTTPS signatures have not been added to the sensor.
C. A DoS policy should be used, instead of an IPS sensor.
D. A DoS policy should be used, instead of an IPS sensor.
E. The firewall policy is not using a full SSL inspection profile.

Answer: E

NEW QUESTION 51
Refer to the exhibit.

Review the Intrusion Prevention System (IPS) profile signature settings. Which statement is correct in adding the FTP.Login.Failed signature to the IPS sensor profile?

A. The signature setting uses a custom rating threshold.
B. The signature setting includes a group of other signatures.
C. Traffic matching the signature will be allowed and logged.
D. Traffic matching the signature will be silently dropped and logged.

Answer: B

NEW QUESTION 56
Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

A. Subject Key Identifiervalue
B. SMMIE Capabilitiesvalue
C. Subjectvalue
D. Subject Alternative Namevalue

Answer: C

NEW QUESTION 58
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view
B. Log backups from the CLI cannot be restored to another FortiGate.
C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

NEW QUESTION 59
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT-6.4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4_FGT-6.4 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT-6.4/

Money Back Guarantee

NSE4_FGT-6.4 Practice Exam Features:

* NSE4_FGT-6.4 Questions and Answers Updated Frequently

* NSE4_FGT-6.4 Practice Questions Verified by Expert Senior Certified Staff

* NSE4_FGT-6.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4_FGT-6.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year