Fortinet

Exam Questions NSE4_FGT-6.4

Fortinet NSE 4 - FortiOS 6.4

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 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 clusteris always assigned IP address 169.254.0.1.

Answer: AB

NEW QUESTION 3
NGFW mode allows policy-based configuration for most inspection rules. Which security profile's configuration does not change when you enable policy-based inspection?

A. Web filtering
B. Antivirus
C. Web proxy
D. Application control

Answer: B

NEW QUESTION 4
Which two protocol options are available on the CLI but not on the GUI when configuring an SD-WAN Performance SLA? (Choose two.)

A. DNS
B. ping
C. udp-echo
D. TWAMP

Answer: AC

NEW QUESTION 5
Examine the network diagram shown in the exhibit, then answer the following question:

Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

A. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
B. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
C. 10.4.200.0/30 is directly connected, port2
D. 172.16.32.0/24 is directly connected, port1

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
Which three statements about a flow-based antivirus profile are correct? (Choose three.)

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

Answer:

CDE

NEW QUESTION 8
Examine this FortiGate configuration:

Examine the output of the following debug command:

Based on the diagnostic outputs above, how is the FortiGate handling the traffic for new sessions that require inspection?

A. It is allowed, but with no inspection
B. It is allowed and inspected as long as the inspection is flow based
C. It is dropped.
D. It is allowed and inspected, as long as the only inspection required is antivirus.

Answer: C

NEW QUESTION 9
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 10
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 sourceusingtheincoming interface.
C. Strict RPF checks only for the existence of at cast one active route back to the source using the incoming interface.
D. Strict RPF allows packets back to sources with all active routes.

Answer: A

NEW QUESTION 10
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 12
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: B

NEW QUESTION 15
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 18
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
C. 10.200.1.1
D. 10.0.1.254

Answer: B

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

NEW QUESTION 21
An administrator has configured outgoing Interface any in a firewall policy. Which statement is true about the policy list view?

A. Policy lookup will be disabled.
B. By Sequence view will be disabled.
C. Search option will be disabled
D. Interface Pair view will be disabled.

Answer: A

NEW QUESTION 25
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 29
Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
B. ADVPN is only supported with IKEv2.
C. Tunnels are negotiated dynamically between spokes.
D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Answer: AC

NEW QUESTION 31
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 internet. TheTo_Internet VDOM is the only VDOM with internet access and is directly connected to ISP modem.
Which two statements are true? (Choose two.)

A. Inter-VDOM links are required to allow traffic between the Local and Root VDOMs.
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 DMZ VDOMs.
D. Inter-VDOM links are not required between the Root and To_Internet VDOMs because the Root VDOM is used only as a management VDOM.

Answer: AD

NEW QUESTION 34
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 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: C

NEW QUESTION 37
An administrator has configured a route-based IPsec VPN between two FortiGate devices. Which statement about this IPsec VPN configuration is true?

A. A phase 2 configuration is not required.
B. This VPN cannot be used as part of a hub-and-spoke topology.
C. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.
D. The IPsec firewall policies must be placed at the top of the list.

Answer: C

Explanation:
In a route-based configuration, FortiGate automatically adds a virtual interface eith the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION 40
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 42
An administrator is configuring an Ipsec between site A and siteB. The Remotes Gateway setting in both sites has been configured as Static IP Address. For site A, the local quick mode selector is 192.16.1.0/24 and the remote quick mode selector is 192.16.2.0/24. How must the administrator configure the local quick mode selector for site B?

A. A.-192.168.3.0/24B.192.168.2.0/24C.192.168.1.0/24D.192.168.0.0/8

Answer: B

NEW QUESTION 45
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 46
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 useraccounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Answer: C

NEW QUESTION 49
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

NEW QUESTION 51
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 Interfac
C. Outgoing Interfac
D. Schedule, and Service fields can be shared with both IPv4and IPv6.
E. The policy table in the GUI can be filtered to display policies with IPv4, IPv6 or IPv4 and IPv6 sources and destinations.
F. The IP version of the sources and destinations in a policy must match.
G. The policy table in the GUI will be consolidated to display policies with IPv4 and IPv6 sources and destinations.

Answer: ACE

NEW QUESTION 55
An administrator observes that the port1 interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

A. The interface has been configured for one-arm sniffer.
B. The interface is a member of a virtual wire pair.
C. The operation mode is transparent.
D. The interface is a member of a zone.
E. Captive portal is enabled in the interface.

Answer: ABC

Explanation:
https://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-whats-new-54/Top_VirtualWirePair.htm

NEW QUESTION 58
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 59
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 63
......

Relate Links

100% Pass Your NSE4_FGT-6.4 Exam with Exambible Prep Materials

https://www.exambible.com/NSE4_FGT-6.4-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/