



Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

About ExamBible

Your Partner of IT Exam

Found in 1998

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

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

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

NEW QUESTION 1

- (Exam Topic 1)

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: BD

Explanation:

Reference: <https://www.skillfulist.com/fortigate/fortigate-conserve-mode-how-to-stop-it-and-what-it-means/>

NEW QUESTION 2

- (Exam Topic 1)

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

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/168495>

Encryption and authentication algorithm needs to match in order for IPSEC be successfully established.

NEW QUESTION 3

- (Exam Topic 1)

An administrator wants to configure timeouts for users. Regardless of the user's behavior, the timer should start as soon as the user authenticates and expire after the configured value.

Which timeout option should be configured on FortiGate?

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

Answer: E

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221#:~:text=Hard%20timeout%3A%20User%20>

NEW QUESTION 4

- (Exam Topic 1)

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

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

Answer: BCE

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.0.0/handbook/265052/logging-and-reporting-overview>

NEW QUESTION 5

- (Exam Topic 1)

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: CD

Explanation:

C: "Operating mode is per-VDOM setting. You can combine transparent mode VDOM's with NAT mode VDOMs on the same physical Fortigate.

D: "Inspection-mode selection has moved from VDOM to firewall policy, and the default inspection-mode is flow, so NGFW Mode can be changed from Profile-base (Default) to Policy-base directly in System > Settings from the VDOM" Page 125 of FortiGate_Infrastructure_6.4_Study_Guide

NEW QUESTION 6

- (Exam Topic 1)

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: D

Explanation:

Action is drop, signature default action is listed only in the signature, it would only match if action was set to default.

NEW QUESTION 7

- (Exam Topic 1)

Which two statements about FortiGate FSSO agentless polling mode are true? (Choose two.)

- A. FortiGate uses the AD server as the collector agent.
- B. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- C. FortiGate does not support workstation check.
- D. FortiGate directs the collector agent to use a remote LDAP server.

Answer: BD

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

NEW QUESTION 8

- (Exam Topic 1)

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. Change Administrator profile
- D. Enable two-factor authentication

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD34502>

NEW QUESTION 9

- (Exam Topic 1)

Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

- A. get system status
- B. get system performance status
- C. diagnose sys top
- D. get system arp

Answer: D

Explanation:

"If you suspect that there is an IP address conflict, or that an IP has been assigned to the wrong device, you may need to look at the ARP table."

NEW QUESTION 10

- (Exam Topic 1)

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 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: A

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46542>

NEW QUESTION 10

- (Exam Topic 1)

Refer to the exhibit.

Given the security fabric topology shown in the exhibit, which two statements are true? (Choose two.)

- A. There are five devices that are part of the security fabric.
- B. Device detection is disabled on all FortiGate devices.
- C. This security fabric topology is a logical topology view.
- D. There are 19 security recommendations for the security fabric.

Answer: CD

Explanation:

References: <https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/761085/results>

<https://docs.fortinet.com/document/fortimanager/6.2.0/new-features/736125/security-fabric-topology>

NEW QUESTION 12

- (Exam Topic 1)

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: BC

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/ports-and-protocols/564712/fgcp-fortigate-clustering-protocol>

NEW QUESTION 16

- (Exam Topic 1)

Refer to the exhibit.

Which contains a session diagnostic output. Which statement is true about the session diagnostic output?

- A. The session is in SYN_SENT state.
- B. The session is in FIN_ACK state.
- C. The session is in FTN_WAIT state.
- D. The session is in ESTABLISHED state.

Answer: A

Explanation:

Indicates TCP (proto=6) session in SYN_SENT state (proto=state=2) <https://kb.fortinet.com/kb/viewContent.do?externalId=FD30042>

NEW QUESTION 21

- (Exam Topic 1)

Which two protocols are used to enable administrator access of a FortiGate device? (Choose two.)

- A. SSH
- B. HTTPS
- C. FTM
- D. FortiTelemetry

Answer: AB

Explanation:

Reference:

<https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/995103/buildingsecurity-into-fortios>

NEW QUESTION 23

- (Exam Topic 1)

Which two statements are correct about SLA targets? (Choose two.)

- A. You can configure only two SLA targets per one Performance SLA.
- B. SLA targets are optional.
- C. SLA targets are required for SD-WAN rules with a Best Quality strategy.
- D. SLA targets are used only when referenced by an SD-WAN rule.

Answer: BD

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/382233/performance-sla-sla-targets>

NEW QUESTION 27

- (Exam Topic 1)

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: CD

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD46328>

NEW QUESTION 29

- (Exam Topic 1)

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 sec configuration-sync local.
- B. Change the csf setting on ISFW (downstream) to sec configuracion-sync local.
- C. Change the csf setting on Local-FortiGate (root) to sec fabric-objecc-unificacion defaultc.
- D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaultc.

Answer: A

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD43820>

NEW QUESTION 34

- (Exam Topic 1)

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 37

- (Exam Topic 1)

Which statement is correct regarding the inspection of some of the services available by web applications embedded in third-party websites?

- A. The security actions applied on the web applications will also be explicitly applied on the third-party websites.
- B. The application signature database inspects traffic only from the original web application server.
- C. FortiGuard maintains only one signature of each web application that is unique.
- D. FortiGate can inspect sub-application traffic regardless where it was originated.

Answer: D

Explanation:

Reference:

https://help.fortinet.com/fortiproxy/11/Content/Admin%20Guides/FPX-AdminGuide/300_System/303d_FortiG

NEW QUESTION 42

- (Exam Topic 2)

View the exhibit:

Which the FortiGate handle web proxy traffic rue? (Choose two.)

- A. Broadcast traffic received in port1-VLAN10 will not be forwarded to port2-VLAN10.
- B. port-VLAN1 is the native VLAN for the port1 physical interface.
- C. port1-VLAN10 and port2-VLAN10 can be assigned to different VDOMs.
- D. Traffic between port1-VLAN1 and port2-VLAN1 is allowed by default.

Answer: AC

NEW QUESTION 44

- (Exam Topic 2)

Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

- A. FortiGate points the collector agent to use a remote LDAP server.
- B. FortiGate uses the AD server as the collector agent.
- C. FortiGate uses the SMB protocol to read the event viewer logs from the DCs.
- D. FortiGate queries AD by using the LDAP to retrieve user group information.

Answer: CD

Explanation:

Fortigate Infrastructure 7.0 Study Guide P.272-273 <https://kb.fortinet.com/kb/documentLink.do?externalID=FD47732>

NEW QUESTION 47

- (Exam Topic 2)

Examine this PAC file configuration.

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

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- 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. Any web request fortinet.com is allowed to bypass the proxy.

Answer: AD

NEW QUESTION 52

- (Exam Topic 2)

Which of the following are purposes of NAT traversal in IPsec? (Choose two.)

- A. To detect intermediary NAT devices in the tunnel path.
- B. To dynamically change phase 1 negotiation mode aggressive mode.
- C. To encapsulation ESP packets in UDP packets using port 4500.
- D. To force a new DH exchange with each phase 2 rekey.

Answer: AC

NEW QUESTION 54

- (Exam Topic 2)

You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.

What is the default behavior when the local disk is full?

- A. Logs are overwritten and the only warning is issued when log disk usage reaches the threshold of 95%.

- B. No new log is recorded until you manually clear logs from the local disk.
- C. Logs are overwritten and the first warning is issued when log disk usage reaches the threshold of 75%.
- D. No new log is recorded after the warning is issued when log disk usage reaches the threshold of 95%.

Answer: C

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/cli-reference/462620/log-disk-setting>

NEW QUESTION 57

- (Exam Topic 2)

To complete the final step of a Security Fabric configuration, an administrator must authorize all the devices on which device?

- A. FortiManager
- B. Root FortiGate
- C. FortiAnalyzer
- D. Downstream FortiGate

Answer: B

NEW QUESTION 59

- (Exam Topic 2)

An administrator has configured two-factor authentication to strengthen SSL VPN access. Which additional best practice can an administrator implement?

- A. Configure Source IP Pools.
- B. Configure split tunneling in tunnel mode.
- C. Configure different SSL VPN realms.
- D. Configure host check.

Answer: D

NEW QUESTION 60

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 63

- (Exam Topic 2)

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 67

- (Exam Topic 2)

Which two statements are true about collector agent standard access mode? (Choose two.)

- A. Standard mode uses Windows convention-NetBios: Domain\Username.
- B. Standard mode security profiles apply to organizational units (OU).
- C. Standard mode security profiles apply to user groups.
- D. Standard access mode supports nested groups.

Answer: AC

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.0.0/handbook/482937/agent-based-fsso>

NEW QUESTION 70

- (Exam Topic 2)

Refer to the exhibit.

The exhibit contains a network diagram, central SNAT policy, and IP pool 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. A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied. Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

- A. 10.200.1.149
- B. 10.200.1.1
- C. 10.200.1.49
- D. 10.200.1.99

Answer: D

NEW QUESTION 74

- (Exam Topic 2)
Refer to the exhibit.

The exhibit shows proxy policies and proxy addresses, the authentication rule and authentication scheme, users, and firewall address. An explicit web proxy is configured for subnet range 10.0.1.0/24 with three explicit web proxy policies. The authentication rule is configured to authenticate HTTP requests for subnet range 10.0.1.0/24 with a form-based authentication scheme for the FortiGate local user database. Users will be prompted for authentication. How will FortiGate process the traffic when the HTTP request comes from a machine with the source IP 10.1.1.10 to the destination <http://www.fortinet.com>? (Choose two.)

- A. If a Mozilla Firefox browser is used with User-B credentials, the HTTP request will be allowed.
- B. If a Google Chrome browser is used with User-B credentials, the HTTP request will be allowed.
- C. If a Mozilla Firefox browser is used with User-A credentials, the HTTP request will be allowed.
- D. If a Microsoft Internet Explorer browser is used with User-B credentials, the HTTP request will be allowed.

Answer: BD

NEW QUESTION 78

- (Exam Topic 2)
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>

NEW QUESTION 81

- (Exam Topic 2)
Which three CLI commands can you use to troubleshoot Layer 3 issues if the issue is in neither the physical layer nor the link layer? (Choose three.)

- A. diagnose sys top
- B. execute ping
- C. execute traceroute
- D. diagnose sniffer packet any
- E. get system arp

Answer: BCD

NEW QUESTION 85

- (Exam Topic 2)
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 90

- (Exam Topic 2)
Exhibit:

Refer to the exhibit to view the authentication rule configuration In this scenario, which statement is true?

- A. IP-based authentication is enabled
- B. Route-based authentication is enabled
- C. Session-based authentication is enabled.
- D. Policy-based authentication is enabled

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD45387>

NEW QUESTION 95

- (Exam Topic 2)

Which of the following statements about central NAT are true? (Choose two.)

- A. IP tool references must be removed from existing firewall policies before enabling central NAT.
- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall.

Answer: AB

NEW QUESTION 98

- (Exam Topic 2)

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: CD

NEW QUESTION 102

- (Exam Topic 2)

Which two VDOMs are the default VDOMs created when FortiGate is set up in split VDOM mode? (Choose two.)

- A. FG-traffic
- B. Mgmt
- C. FG-Mgmt
- D. Root

Answer: AD

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/758820/split-task-vdom-mode>

NEW QUESTION 106

- (Exam Topic 2)

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

Answer: B

NEW QUESTION 107

- (Exam Topic 2)

In an explicit proxy setup, where is the authentication method and database configured?

- A. Proxy Policy
- B. Authentication Rule
- C. Firewall Policy
- D. Authentication scheme

Answer: D

NEW QUESTION 111

- (Exam Topic 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 browser requires a software update.
- B. FortiGate does not support full SSL inspection when web filtering is enabled.
- C. The CA certificate set on the SSL/SSH inspection profile has not been imported into the browser.
- D. There are network connectivity issues.

Answer: C

Explanation:

Reference: <https://kb.fortinet.com/kb/documentLink.do?externalID=FD41394>

NEW QUESTION 114

- (Exam Topic 2)

Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

- A. Root VDOM
- B. FG-traffic VDOM
- C. Customer VDOM
- D. Global VDOM

Answer: A

NEW QUESTION 118

- (Exam Topic 2)

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: A

Explanation:

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

NEW QUESTION 121

- (Exam Topic 2)

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip_src_session
- D. Location: server Protocol: SMTP

Answer: B

NEW QUESTION 122

- (Exam Topic 2)

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 124

- (Exam Topic 2)

Which of the following are valid actions for FortiGuard category based filter in a web filter profile ui proxy-based inspection mode? (Choose two.)

- A. Warning
- B. Exempt
- C. Allow
- D. Learn

Answer: AC

NEW QUESTION 128

- (Exam Topic 2)

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 with the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION 131

- (Exam Topic 2)

Which two statements are 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 clicking 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 all FortiGate devices.

Answer: BC

Explanation:

Reference: <https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/292634/security-rating>

NEW QUESTION 135

- (Exam Topic 2)

Examine this output from a debug flow:

Why did the FortiGate drop the packet?

- A. The next-hop IP address is unreachable.
- B. It failed the RPF check.
- C. It matched an explicitly configured firewall policy with the action DENY.
- D. It matched the default implicit firewall policy.

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=13900>

NEW QUESTION 140

- (Exam Topic 2)

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 145

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 148

- (Exam Topic 2)

Which three statements about security associations (SA) in IPsec are correct? (Choose three.)

- A. Phase 2 SAs are used for encrypting and decrypting the data exchanged through the tunnel.
- B. An SA never expires.
- C. A phase 1 SA is bidirectional, while a phase 2 SA is directional.
- D. Phase 2 SA expiration can be time-based, volume-based, or both.
- E. Both the phase 1 SA and phase 2 SA are bidirectional.

Answer: ACD

NEW QUESTION 149

- (Exam Topic 2)

Refer to the exhibit.

The exhibits show a network diagram and the explicit web proxy configuration.

In the command diagnose sniffer packet, what filter can you use to capture the traffic between the client and the explicit web proxy?

- A. 'host 192.168.0.2 and port 8080'
- B. 'host 10.0.0.50 and port 80'
- C. 'host 192.168.0.1 and port 80'
- D. 'host 10.0.0.50 and port 8080'

Answer: A

NEW QUESTION 154

- (Exam Topic 2)

Which three statements are true regarding session-based authentication? (Choose three.)

- A. HTTP sessions are treated as a single user.
- B. IP sessions from the same source IP address are treated as a single user.
- C. It can differentiate among multiple clients behind the same source IP address.
- D. It requires more resources.
- E. It is not recommended if multiple users are behind the source NAT

Answer: ACD

NEW QUESTION 156

- (Exam Topic 2)

Refer to the exhibit to view the application control profile.

Users who use Apple FaceTime video conferences are unable to set up meetings. In this scenario, which statement is true?

- A. Apple FaceTime belongs to the custom monitored filter.
- B. The category of Apple FaceTime is being monitored.
- C. Apple FaceTime belongs to the custom blocked filter.
- D. The category of Apple FaceTime is being blocked.

Answer: C

NEW QUESTION 158

- (Exam Topic 2)

Why does FortiGate keep TCP sessions in the session table for some seconds even after both sides (client and server) have terminated the session?

- A. To remove the NAT operation.
- B. To generate logs
- C. To finish any inspection operations.
- D. To allow for out-of-order packets that could arrive after the FIN/ACK packets.

Answer: D

NEW QUESTION 160

.....

Relate Links

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

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

Contact us

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

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