Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

https://www.2passeasy.com/dumps/NSE4_FGT-7.0/

NEW QUESTION 1
- (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 2
- (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 3
- (Exam Topic 1)
Which type of logs on FortiGate record information about traffic directly to and from the FortiGate management IP addresses?

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

Answer: C

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/5.4.0/cookbook/476970

NEW QUESTION 4
- (Exam Topic 1)
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. The action on firewall policy ID 1 is set to warning.
C. Access to the social networking web filter category was explicitly blocked to all users.
D. The name of the firewall policy is all_users_web.

Answer: A

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
When configuring a firewall virtual wire pair policy, which following statement is true?

A. Any number of virtual wire pairs can be included, as long as the policy traffic direction is the same.
B. Only a single virtual wire pair can be included in each policy.
C. Any number of virtual wire pairs can be included in each policy, regardless of the policy traffic direction settings.
D. Exactly two virtual wire pairs need to be included in each policy.

Answer: A

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48690

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
FortiGuard categories can be overridden and defined in different categories. To create a web rating override for example.com home page, the override must be configured using a specific syntax.
Which two syntaxes are correct to configure web rating for the home page? (Choose two.)

A. www.example.com:443
B. www.example.com
C. example.com
D. www.example.com/index.html

Answer: BC

Explanation:
FortiGate_Security_6.4 page 384
When using FortiGuard category filtering to allow or block access to a website, one option is to make a web rating override and define the website in a different category. Web ratings are only for host names— "no URLs or wildcard characters are allowed".

NEW QUESTION 9
- (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 10
- (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 10
- (Exam Topic 1)
Which two statements are correct about NGFW Policy-based mode? (Choose two.)

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

Answer: CD

NEW QUESTION 13
- (Exam Topic 1)
Refer to the exhibit.

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster. Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.
B. FortiGate devices are not in sync because one device is down.
C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.
D. FortiGate SN FGVM010000064692 has the higher HA priority.

Answer: AD

Explanation:
* 1. Override is disable by default - OK
* 2. "If the HA uptime of a device is AT LEAST FIVE MINUTES (300 seconds) MORE than the HA Uptime of the other FortiGate devices, it becomes the primary"

The question here is : HA Uptime of FGVM01000006492 > 5 minutes? NO - 198 seconds < 300 seconds (5 minutes) Page 314 Infra Study Guide.
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/666653/primary-unit-selection-with-override-disab

NEW QUESTION 15
- (Exam Topic 1)
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: A

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/232929/troubleshooting-high-cpu-usage

NEW QUESTION 16
- (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 17
- (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 20
- (Exam Topic 2)
View the exhibit.

A user behind the FortiGate is trying to go to http://www.addictinggames.com (Addicting Games). Based on this configuration, which statement is true?

A. Addicting.Games is allowed based on the Application Overrides configuration.
B. Addicting.Games is blocked on the Filter Overrides configuration.
C. Addicting.Games can be allowed only if the Filter Overrides actions is set to Exempt.
D. Addcting.Games is allowed based on the Categories configuration.

Answer: A

NEW QUESTION 23
- (Exam Topic 2)
FortiGate is configured as a policy-based next-generation firewall (NGFW) and is applying web filtering and application control directly on the security policy.
Which two other security profiles can you apply to the security policy? (Choose two.)

A. Antivirus scanning
B. File filter
C. DNS filter
D. Intrusion prevention

Answer: AD

NEW QUESTION 26
- (Exam Topic 2)
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 28
- (Exam Topic 2)
Which feature in the Security Fabric takes one or more actions based on event triggers?

A. Fabric Connectors
B. Automation Stitches

C. Security Rating
D. Logical Topology

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/286973/fortinet-security-fabric

NEW QUESTION 30
- (Exam Topic 2)
Refer to the exhibit.

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

Answer: AD

NEW QUESTION 35
- (Exam Topic 2)
The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile.
What order must FortiGate use when the web filter profile has features enabled, such as safe search?

A. DNS-based web filter and proxy-based web filter
B. Static URL filter, FortiGuard category filter, and advanced filters
C. Static domain filter, SSL inspection filter, and external connectors filters
D. FortiGuard category filter and rating filter

Answer: B

Explanation:
Reference: https://fortinet121.rssing.com/chan-67705148/all_p1.html

NEW QUESTION 36
- (Exam Topic 2)
Which CLI command will display sessions both from client to the proxy and from the proxy to the servers?

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

Answer: A

NEW QUESTION 37

- (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 40
- (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 41
- (Exam Topic 2)
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 46
- (Exam Topic 2)
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

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD50220

NEW QUESTION 50
- (Exam Topic 2)
If the Services field is configured in a Virtual IP (VIP), which statement is true when central NAT is used?

A. The Services field prevents SNAT and DNAT from being combined in the same policy.
B. The Services field is used when you need to bundle several VIPs into VIP groups.
C. The Services field removes the requirement to create multiple VIPs for different services.
D. The Services field prevents multiple sources of traffic from using multiple services to connect to a singlecomputer.

Answer: C

NEW QUESTION 51
- (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 54
- (Exam Topic 2)
Refer to the exhibit.

The exhibit shows a CLI output of firewall policies, proxy policies, and proxy addresses.
How does FortiGate process the traffic sent to http://www.fortinet.com?

A. Traffic will be redirected to the transparent proxy and it will be allowed by proxy policy ID 3.
B. Traffic will not be redirected to the transparent proxy and it will be allowed by firewall policy ID 1.
C. Traffic will be redirected to the transparent proxy and It will be allowed by proxy policy ID 1.
D. Traffic will be redirected to the transparent proxy and it will be denied by the proxy implicit deny policy.

Answer: D

NEW QUESTION 59
- (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 61
- (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 eith the VPN name (Infrastructure Study Guide, 206)

NEW QUESTION 63
- (Exam Topic 2)
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 scanning of application traffic to the DNS protocol only.
B. It limits the scanning of application traffic to use parent signatures only.
C. It limits the scanning of application traffic to the browser-based technology category only.
D. It limits the scanning of application traffic to the application category only.

Answer: C

NEW QUESTION 66
- (Exam Topic 2)
Which of the following statements correctly describes FortiGates route lookup behavior when searching for a suitable gateway? (Choose two)

A. Lookup is done on the first packet from the session originator
B. Lookup is done on the last packet sent from the responder
C. Lookup is done on every packet, regardless of direction
D. Lookup is done on the trust reply packet from the responder

Answer: AD

NEW QUESTION 68
- (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 73
- (Exam Topic 2)
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 74
- (Exam Topic 2)
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: AB

NEW QUESTION 78
- (Exam Topic 2)
Examine the following web filtering log.

Which statement about the log message is true?

A. The action for the category Games is set to block.
B. The usage quota for the IP address 10.0.1.10 has expired
C. The name of the applied web filter profile is default.
D. The web site miniclip.com matches a static URL filter whose action is set to Warning.

Answer: C

NEW QUESTION 80
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4_FGT-7.0 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-7.0 Product From:

https://www.2passeasy.com/dumps/NSE4_FGT-7.0/

Money Back Guarantee

NSE4_FGT-7.0 Practice Exam Features:

* NSE4_FGT-7.0 Questions and Answers Updated Frequently

* NSE4_FGT-7.0 Practice Questions Verified by Expert Senior Certified Staff

* NSE4_FGT-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4_FGT-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year