Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

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)
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 3
- (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 4
- (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 5
- (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 6
- (Exam Topic 1)
An administrator wants to configure Dead Peer Detection (DPD) on IPSEC VPN for detecting dead tunnels. The requirement is that FortiGate sends DPD probes only when no traffic is observed in the tunnel.
Which DPD mode on FortiGate will meet the above requirement?

A. Disabled
B. On Demand
C. Enabled
D. On Idle

Answer: D

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD40813

NEW QUESTION 7
- (Exam Topic 1)
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 allow attackers matching the NTP.Spoofed.KoD.DoS signature.
B. The sensor will block all attacks aimed at Windows servers.
C. The sensor will reset all connections that match these signatures.
D. The sensor will gather a packet log for all matched traffic.

Answer: AB

NEW QUESTION 8
- (Exam Topic 1)
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 Detection Mode setting is not set to Passive.
B. Administrator didn't configure a gateway for the SD-WAN members, or configured gateway is not valid.
C. The configured participants are not SD-WAN members.
D. The Enable probe packets setting is not enabled.

Answer: BD

NEW QUESTION 9
- (Exam Topic 1)
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 highest distance.
B. The port3 default route has the lowest metric.
C. There will be eight routes active in the routing table.
D. The port1 and port2 default routes are active in the routing table.

Answer: AD

NEW QUESTION 10
- (Exam Topic 1)

Which two statements about antivirus scanning mode are true? (Choose two.)

A. In proxy-based inspection mode, files bigger than the buffer size are scanned.
B. In flow-based inspection mode, FortiGate buffers the file, but also simultaneously transmits it to the client.
C. In proxy-based inspection mode, antivirus scanning buffers the whole file for scanning, before sending it to the client.
D. In flow-based inspection mode, files bigger than the buffer size are scanned.

Answer: BC

Explanation:
An antivirus profile in full scan mode buffers up to your specified file size limit. The default is 10 MB. That is large enough for most files, except video files. If your FortiGate model has more RAM, you may be able to increase this threshold. Without a limit, very large files could exhaust the scan memory. So, this threshold balances risk and performance. Is this tradeoff unique to FortiGate, or to a specific model? No. Regardless of vendor or model, you must make a choice. This is because of the difference between scans in theory, that have no limits, and scans on real-world devices, that have finite RAM. In order to detect 100% of malware regardless of file size, a firewall would need infinitely large RAM—something that no device has in the real world. Most viruses are very small. This table shows a typical tradeoff. You can see that with the default 10 MB threshold, only 0.01% of viruses pass through.

NEW QUESTION 10
- (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 14
- (Exam Topic 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 firewall policy allowed the connection.
C. A new traffic session is created.
D. The default route is required to receive a reply.

Answer: AC

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/54688/debugging-the-packet-flow

NEW QUESTION 17
- (Exam Topic 1)
Which engine handles application control traffic on the next-generation firewall (NGFW) FortiGate?

A. Antivirus engine
B. Intrusion prevention system engine
C. Flow engine
D. Detection engine

Answer: B

Explanation:
Reference: http://docs.fortinet.com/document/fortigate/6.0.0/handbook/240599/application-control

NEW QUESTION 18
- (Exam Topic 1)
Which two attributes are required on a certificate so it can be used as a CA certificate on SSL Inspection? (Choose two.)

A. The keyUsage extension must be set to keyCertSign.
B. The common name on the subject field must use a wildcard name.
C. The issuer must be a public CA.
D. The CA extension must be set to TRUE.

Answer: AD

Explanation:
Reference: https://www.reddit.com/r/fortinet/comments/c7j6jg/recommended_ssl_cert/

NEW QUESTION 20
- (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 21
- (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 26
- (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 28
- (Exam Topic 1)
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 192.168.1.0/24 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: C

NEW QUESTION 29
- (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 31
- (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 32
- (Exam Topic 1)
How does FortiGate act when using SSL VPN in web mode?

A. FortiGate acts as an FDS server.
B. FortiGate acts as an HTTP reverse proxy.
C. FortiGate acts as DNS server.
D. FortiGate acts as router.

Answer: B

Explanation:
Reference:
https://pub.kb.fortinet.com/ksmcontent/Fortinet-Public/current/Fortigate_v4.0MR3/fortigate-sslvpn-40-mr3.pdf

NEW QUESTION 36
- (Exam Topic 1)
Refer to the exhibits.

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

Answer: A

Explanation:
The lock logo behind Facebook_like.Button indicates that SSL Deep Inspection is Required.

NEW QUESTION 41
- (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 46
- (Exam Topic 1)
Refer to the exhibit.

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

A. Traffic between port2 and port2-vlan1 is allowed by default.
B. port1-vlan10 and port2-vlan10 are part of the same broadcast domain.
C. port1 is a native VLAN.
D. port1-vlan and port2-vlan1 can be assigned in the same VDOM or to different VDOMs.

Answer: CD

Explanation:
https://community.fortinet.com/t5/FortiGate/Technical-Tip-rules-about-VLAN-configuration-and-VDOM-interf
https://kb.fortinet.com/kb/viewContent.do?externalId=FD30883

NEW QUESTION 49
- (Exam Topic 2)
Refer to the exhibit.

In the network shown in the exhibit, the web client cannot connect to the HTTP web server. The administrator runs the FortiGate built-in sniffer and gets the output as shown in the exhibit.
What should the administrator do next to troubleshoot the problem?

A. Run a sniffer on the web server.
B. Capture the traffic using an external sniffer connected to port1.
C. Execute another sniffer in the FortiGate, this time with the filter “host 10.0.1.10”
D. Execute a debug flow.

Answer: D

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

The exhibit contains a network interface configuration, firewall policies, and a CLI console configuration. How will FortiGate handle user authentication for traffic that arrives on the LAN interface?

A. If there is a full-through policy in place, users will not be prompted for authentication.
B. Users from the Sales group will be prompted for authentication and can authenticate successfully with the correct credentials.
C. Authentication is enforced at a policy level; all users will be prompted for authentication.
D. Users from the HR group will be prompted for authentication and can authenticate successfully with the correct credentials.

Answer: C

NEW QUESTION 59
- (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 60
- (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 65
- (Exam Topic 2)
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 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.
B. 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.

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 203.0.114.24/32 through port3.

Answer: D

NEW QUESTION 70
- (Exam Topic 2)
What devices form the core of the security fabric?

A. Two FortiGate devices and one FortiManager device
B. One FortiGate device and one FortiManager device
C. Two FortiGate devices and one FortiAnalyzer device
D. One FortiGate device and one FortiAnalyzer device

Answer: C

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/425100/components

NEW QUESTION 74
- (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 78
- (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 82
- (Exam Topic 2)
Refer to the exhibit.

The exhibit contains a network diagram, firewall policies, and a firewall address object configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-user2. Remote-user2 is still able to access Webserver.
Which two changes can the administrator make to deny Webserver access for Remote-User2? (Choose two.)

A. Disable match-vip in the Deny policy.
B. Set the Destination address as Deny_IP in the Allow-access policy.
C. Enable match vip in the Deny policy.
D. Set the Destination address as Web_server in the Deny policy.

Answer: CD

NEW QUESTION 85
- (Exam Topic 2)
A FortiGate is operating in NAT mode and configured with two virtual LAN (VLAN) sub interfaces added to the physical interface.
Which statements about the VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.

A. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in different subnets.
B. The two VLAN sub interfaces must have different VLAN IDs.
C. The two VLAN sub interfaces can have the same VLAN ID, only if they belong to different VDOMs.
D. The two VLAN sub interfaces can have the same VLAN ID, only if they have IP addresses in the same subnet.

Answer: B

Explanation:
FortiGate_Infrastructure_6.0_Study_Guide_v2-Online.pdf –> page 147
“Multiple VLANs can coexist in the same physical interface, provide they have different VLAN ID”

NEW QUESTION 89

- (Exam Topic 2)
Refer to the exhibit, which contains a session diagnostic output.

Which statement is true about the session diagnostic output?

A. The session is a UDP unidirectional state.
B. The session is in TCP ESTABLISHED state.
C. The session is a bidirectional UDP connection.
D. The session is a bidirectional TCP connection.

Answer: C

NEW QUESTION 90
- (Exam Topic 2)
Which two statements are correct about a software switch on FortiGate? (Choose two.)

A. It can be configured only when FortiGate is operating in NAT mode
B. Can act as a Layer 2 switch as well as a Layer 3 router
C. All interfaces in the software switch share the same IP address
D. It can group only physical interfaces

Answer: AC

NEW QUESTION 93
- (Exam Topic 2)
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 98
- (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 101
- (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 104
- (Exam Topic 2)
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, based on the Apple filter configuration.
C. Apple FaceTime will be allowed only if the filter in Application and Filter Overrides is set to Learn
D. Apple FaceTime will be allowed, based on the Categories configuration.

Answer: A

NEW QUESTION 108
- (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 110
- (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 113
- (Exam Topic 2)
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 114
- (Exam Topic 2)
If Internet Service is already selected as Destination in a firewall policy, which other configuration objects can be selected to the Destination field of a firewall policy?

A User or User Group

A. IP address
B. No other object can be added
C. FQDN address

Answer: B

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy

NEW QUESTION 115
- (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 116
- (Exam Topic 2)
Refer to the exhibit, which contains a radius server configuration.

An administrator added a configuration for a new RADIUS server. While configuring, the administrator selected the Include in every user group option.
What will be the impact of using Include in every user group option in a RADIUS configuration?

A. This option places the RADIUS server, and all users who can authenticate against that server, into every FortiGate user group.
B. This option places all FortiGate users and groups required to authenticate into the RADIUS server, which, in this case, is FortiAuthenticator.
C. This option places all users into every RADIUS user group, including groups that are used for the LDAP server on FortiGate.
D. This option places the RADIUS server, and all users who can authenticate against that server, into every RADIUS group.

Answer: A

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/634373/authentication-servers

NEW QUESTION 118
- (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 121
- (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 124
- (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 127
- (Exam Topic 2)
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 132
- (Exam Topic 2)
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 public key of the web server certificate must be installed on the browser.
B. The web-server certificate must be installed on the browser.
C. The CA certificate that signed the web-server certificate must be installed on the browser.
D. The private key of the CA certificate that signed the browser certificate must be installed on the browser.

Answer: C

NEW QUESTION 135
- (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 139
- (Exam Topic 2)
Refer to the exhibit.

Which contains a Performance SLA 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

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/478384/performance-sla-linkmonitoring

NEW QUESTION 144
- (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 145
- (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 148
- (Exam Topic 2)
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: ABE

NEW QUESTION 152
- (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 154
- (Exam Topic 2)
What types of traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

A. Traffic to botnetservers
B. Traffic to inappropriate web sites
C. Server information disclosure attacks
D. Credit card data leaks
E. SQL injection attacks

Answer: CDE

NEW QUESTION 158
- (Exam Topic 2)
Which three methods are used by the collector agent for AD polling? (Choose three.)

A. FortiGate polling
B. NetAPI
C. Novell API
D. WMI
E. WinSecLog

Answer: BDE

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

NEW QUESTION 162
- (Exam Topic 2)
Which three criteria can a FortiGate use to look for a matching firewall policy to process traffic? (Choose three.)

A. Source defined as Internet Services in the firewall policy.
B. Destination defined as Internet Services in the firewall policy.

C. Highest to lowest priority defined in the firewall policy.
D. Services defined in the firewall policy.
E. Lowest to highest policy ID number.

Answer: ABD

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD47435

NEW QUESTION 163
- (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 168
- (Exam Topic 2)
What is the primary FortiGate election process when the HA override setting is disabled?

A. Connected monitored ports > System uptime > Priority > FortiGate Serial number
B. Connected monitored ports > HA uptime > Priority > FortiGate Serial number
C. Connected monitored ports > Priority > HA uptime > FortiGate Serial number
D. Connected monitored ports > Priority > System uptime > FortiGate Serial number

Answer: B

Explanation:
Reference: http://myitmicroblog.blogspot.com/2018/11/what-should-you-know-about-ha-override.html

NEW QUESTION 171
- (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 172
- (Exam Topic 2)
If Internet Service is already selected as Source in a firewall policy, which other configuration objects can be added to the Source filed of a firewall policy?

A. IP address
B. Once Internet Service is selected, no other object can be added
C. User or User Group
D. FQDN address

Answer: B

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.5/cookbook/179236/using-internet-service-in-policy

NEW QUESTION 177
- (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 182
- (Exam Topic 2)
Which security feature does FortiGate provide to protect servers located in the internal networks from attacks such as SQL injections?

A. Denial of Service
B. Web application firewall
C. Antivirus
D. Application control

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortiweb/6.3.3/administration-guide/60895/introduction

NEW QUESTION 186
- (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 191
- (Exam Topic 2)
Which two statements are true about collector agent advanced mode? (Choose two.)

A. Advanced mode uses Windows convention—NetBios: Domain\Username.
B. FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate
C. Advanced mode supports nested or inherited groups
D. Security profiles can be applied only to user groups, not individual users.

Answer: BC

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

NEW QUESTION 193
- (Exam Topic 2)
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 198
- (Exam Topic 2)
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 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 alt FortiGate devices.

Answer: BC

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

NEW QUESTION 201
- (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 205
- (Exam Topic 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: BD

NEW QUESTION 208
- (Exam Topic 2)
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 209
- (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 212
- (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 213
- (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 218
- (Exam Topic 2)
Which statements about the firmware upgrade process on an active-active HA cluster are true? (Choose two.)

A. The firmware image must be manually uploaded to each FortiGate.
B. Only secondary FortiGate devices are rebooted.
C. Uninterruptable upgrade is enabled by default.
D. Traffic load balancing is temporally disabled while upgrading the firmware.

Answer: CD

NEW QUESTION 220
- (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 225
- (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 226
- (Exam Topic 2)
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 227
- (Exam Topic 2)
How do you format the FortiGate flash disk?

A. Load a debug FortiOS image.
B. Load the hardware test (HQIP) image.
C. Execute the CLI command execute formatlogdisk.
D. Select the format boot device option from the BIOS menu.

Answer: D

NEW QUESTION 229
- (Exam Topic 2)
Examine the two static routes shown in the exhibit, then answer the following question.

Which of the following is the expected FortiGate behavior regarding these two routes to the same destination?

A. FortiGate will load balance all traffic across both routes.
B. FortiGate will use the port1 route as the primary candidate.
C. FortiGate will route twice as much traffic to the port2 route
D. FortiGate will only actuate the port1 route in the routing table

Answer: B

Explanation:
“If multiple static routes have the same distance, they are all active; however, only the one with the lowest priority is considered the best path.”

NEW QUESTION 233
- (Exam Topic 2)
What inspection mode does FortiGate use if it is configured as a policy-based next-generation firewall (NGFW)?

A. Full Content inspection
B. Proxy-based inspection
C. Certificate inspection
D. Flow-based inspection

Answer: D

NEW QUESTION 237
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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