Fortinet

Exam Questions NSE4_FGT-7.0

Fortinet NSE 4 - FortiOS 7.0

NEW QUESTION 1
- (Exam Topic 1)
Refer to the exhibits to view the firewall policy (Exhibit A) and the antivirus profile (Exhibit B).

Which statement is correct if a user is unable to receive a block replacement message when downloading an infected file for the first time?

A. The firewall policy performs the full content inspection on the file.
B. The flow-based inspection is used, which resets the last packet to the user.
C. The volume of traffic being inspected is too high for this model of FortiGate.
D. The intrusion prevention security profile needs to be enabled when using flow-based inspection mode.

Answer: B

Explanation:
• "ONLY" If the virus is detected at the "START" of the connection, the IPS engine sends the block replacement message immediately
• When a virus is detected on a TCP session (FIRST TIME), but where "SOME PACKETS" have been already forwarded to the receiver, FortiGate "resets the connection" and does not send the last piece of the file. Although the receiver got most of the file content, the file has been truncated and therefore, can't be opened. The IPS engine also caches the URL of the infected file, so that if a "SECOND ATTEMPT" to transmit the file is made, the IPS engine will then send a block replacement message to the client instead of scanning the file again.
In flow mode, the FortiGate drops the last packet killing the file. But because of that the block replacement message cannot be displayed. If the file is attempted to download again the block message will be shown.

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)
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 6
- (Exam Topic 1)
Which statement correctly describes NetAPI polling mode for the FSSO collector agent?

A. The collector agent uses a Windows API to query DCs for user logins.
B. NetAPI polling can increase bandwidth usage in large networks.
C. The collector agent must search security event logs.
D. The NetSession Enum function is used to track user logouts.

Answer: D

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD34906
https://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&docType=kc&externalId=FD34906&sliceId=1

NEW QUESTION 7
- (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 8
- (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 9
- (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 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)
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 source using the incoming 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: B

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

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 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)
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: D

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD47821

NEW QUESTION 22
- (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 27
- (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 30
- (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 35
- (Exam Topic 1)
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 user accounts to Active Directory (AD).
C. Add user accounts to the FortiGate group fitter.
D. Add user accounts to the Ignore User List.

Answer: D

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD38828

NEW QUESTION 40
- (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 42
- (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 44
- (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 46
- (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 50
- (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 51
- (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 defaulc.
D. Change the csf setting on ISFW (downstream) to sec fabric-objecc-unificacion defaulc.

Answer: A

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

NEW QUESTION 52
- (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 55
- (Exam Topic 1)
A network administrator has enabled SSL certificate inspection and antivirus on FortiGate. When downloading an EICAR test file through HTTP, FortiGate detects the virus and blocks the file. When downloading the same file through HTTPS, FortiGate does not detect the virus and the file can be downloaded.
What is the reason for the failed virus detection by FortiGate?

A. Application control is not enabled
B. SSL/SSH Inspection profile is incorrect
C. Antivirus profile configuration is incorrect
D. Antivirus definitions are not up to date

Answer: B

Explanation:
https traffic requires SSL decryption. Check the ssh inspection profile

NEW QUESTION 59
- (Exam Topic 2)
Which two statements are true when FortiGate is in transparent mode? (Choose two.)

A. By default, all interfaces are part of the same broadcast domain.
B. The existing network IP schema must be changed when installing a transparent mode.
C. Static routes are required to allow traffic to the next hop.
D. FortiGate forwards frames without changing the MAC address.

Answer: AD

Explanation:
Reference: https://kb.fortinet.com/kb/viewAttachment.do?
attachID=Fortigate_Transparent_Mode_Technical_Guide_FortiOS_4_0_version1.2.pdf&documentID=FD33113

NEW QUESTION 62
- (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 63
- (Exam Topic 2)
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. 192.168.3.0/24
B. 192.168.2.0/24
C. 192.168.1.0/24
D. 192.168.0.0/8

Answer: B

NEW QUESTION 64
- (Exam Topic 2)
Refer to the FortiGuard connection debug output.

Based on the output shown in the exhibit, which two statements are correct? (Choose two.)

A. A local FortiManager is one of the servers FortiGate communicates with.
B. One server was contacted to retrieve the contract information.
C. There is at least one server that lost packets consecutively.
D. FortiGate is using default FortiGuard communication settings.

Answer: BD

NEW QUESTION 66
- (Exam Topic 2)
An administrator must disable RPF check to investigate an issue.
Which method is best suited to disable RPF without affecting features like antivirus and intrusion prevention system?

A. Enable asymmetric routing, so the RPF check will be bypassed.
B. Disable the RPF check at the FortiGate interface level for the source check.
C. Disable the RPF check at the FortiGate interface level for the reply check.
D. Enable asymmetric routing at the interface level.

Answer: B

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

NEW QUESTION 69
- (Exam Topic 2)
An administrator has a requirement to keep an application session from timing out on port 80. What two changes can the administrator make to resolve the issue without affecting any existing services running through FortiGate? (Choose two.)

A. Create a new firewall policy with the new HTTP service and place it above the existing HTTP policy.
B. Create a new service object for HTTP service and set the session TTL to never
C. Set the TTL value to never under config system-ttl

D. Set the session TTL on the HTTP policy to maximum

Answer: BC

NEW QUESTION 70
- (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 71
- (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 72
- (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 77
- (Exam Topic 2)
Which three pieces of information does FortiGate use to identify the hostname of the SSL server when SSL certificate inspection is enabled? (Choose three.)

A. The subject field in the server certificate
B. The serial number in the server certificate
C. The server name indication (SNI) extension in the client hello message
D. The subject alternative name (SAN) field in the server certificate
E. The host field in the HTTP header

Answer: ACD

Explanation:
Reference: https://checkthefirewall.com/blogs/fortinet/ssl-inspection

NEW QUESTION 82
- (Exam Topic 2)
Which two statements are true about the RPF check? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.
B. The RPF check is run on the first reply packet of any new session.
C. The RPF check is run on the first sent and reply packet of any new session.
D. RPF is a mechanism that protects FortiGate and your network from IP spoofing attacks.

Answer: AD

Explanation:
Reference: https://www.programmersought.com/article/16383871634/

NEW QUESTION 84
- (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 86
- (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 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 93
- (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 94
- (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 99
- (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)
Refer to the exhibit to view the firewall policy.

Which statement is correct if well-known viruses are not being blocked?

A. The firewall policy does not apply deep content inspection.
B. The firewall policy must be configured in proxy-based inspection mode.
C. The action on the firewall policy must be set to deny.
D. Web filter should be enabled on the firewall policy to complement the antivirus profile.

Answer: A

NEW QUESTION 104
- (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 106
- (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 108
- (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 110
- (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 114
- (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 119
- (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 124
- (Exam Topic 2)
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

Explanation:
https://docs.fortinet.com/document/fortigate/6.0.0/handbook/49719/configuring-sd-wan-load-balancing

NEW QUESTION 128
- (Exam Topic 2)
In which two ways can RPF checking be disabled? (Choose two)

A. Enable anti-replay in firewall policy.
B. Disable the RPF check at the FortiGate interface level for the source check
C. Enable asymmetric routing.
D. Disable strict-arc-check under system settings.

Answer: CD

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD33955

NEW QUESTION 133
- (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 138
- (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 141
- (Exam Topic 2)
Refer to the exhibit.

Based on the raw log, which two statements are correct? (Choose two.)

A. Traffic is blocked because Action is set to DENY in the firewall policy.
B. Traffic belongs to the root VDOM.
C. This is a security log.
D. Log severity is set to error on FortiGate.

Answer: AC

NEW QUESTION 142
- (Exam Topic 2)
Which two policies must be configured to allow traffic on a policy-based next-generation firewall (NGFW) FortiGate? (Choose two.)

A. Firewall policy
B. Policy rule
C. Security policy
D. SSL inspection and authentication policy

Answer: CD

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/5.6.0/cookbook/38324/ngfw-policy-based-mode

NEW QUESTION 145
- (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 146
- (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 147
- (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 151
- (Exam Topic 2)
Which Security rating scorecard helps identify configuration weakness and best practice violations in your network?

A. Fabric Coverage
B. Automated Response
C. Security Posture
D. Optimization

Answer: C

Explanation:
Reference:
https://www.fortinet.com/content/dam/fortinet/assets/support/fortinet-recommended-security-bestpractices.pdf

NEW QUESTION 153
- (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 155
- (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 159
- (Exam Topic 2)
Consider the topology:
Application on a Windows machine <--{SSL VPN} -->FGT--> Telnet to Linux server.
An administrator is investigating a problem where an application establishes a Telnet session to a Linux server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.
The administrator has already verified that the issue is not caused by the application or Linux server. This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.
What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

A. Set the maximum session TTL value for the TELNET service object.
B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.
C. Create a new service object for TELNET and set the maximum session TTL.
D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer: CD

NEW QUESTION 162
- (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 166
- (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 171
- (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 174
- (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 179
- (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 180
- (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 183
- (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 186
- (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 189
- (Exam Topic 2)
Which scanning technique on FortiGate can be enabled only on the CLI?

A. Heuristics scan
B. Trojan scan
C. Antivirus scan
D. Ransomware scan

Answer: A

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/567568/enabling-scanning

NEW QUESTION 191
- (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 196
- (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 199
- (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 204
- (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 208
- (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 211
- (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 215
- (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 220
- (Exam Topic 2)
Which statement about the IP authentication header (AH) used by IPsec is true?

A. AH does not provide any data integrity or encryption.
B. AH does not support perfect forward secrecy.
C. AH provides data integrity bur no encryption.
D. AH provides strong data integrity but weak encryption.

Answer: C

NEW QUESTION 221
- (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 225
- (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 229
- (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 233
- (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 235
- (Exam Topic 2)
Refer to the exhibit, which contains a static route configuration.

An administrator created a static route for Amazon Web Services. What CLI command must the administrator use to view the route?

A. get router info routing-table all
B. get internet service route list
C. get router info routing-table database
D. diagnose firewall proute list

Answer: D

Explanation:

Reference: https://docs.fortinet.com/document/fortigate/latest/administration-guide/139692/routing-concepts

NEW QUESTION 238

.....

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