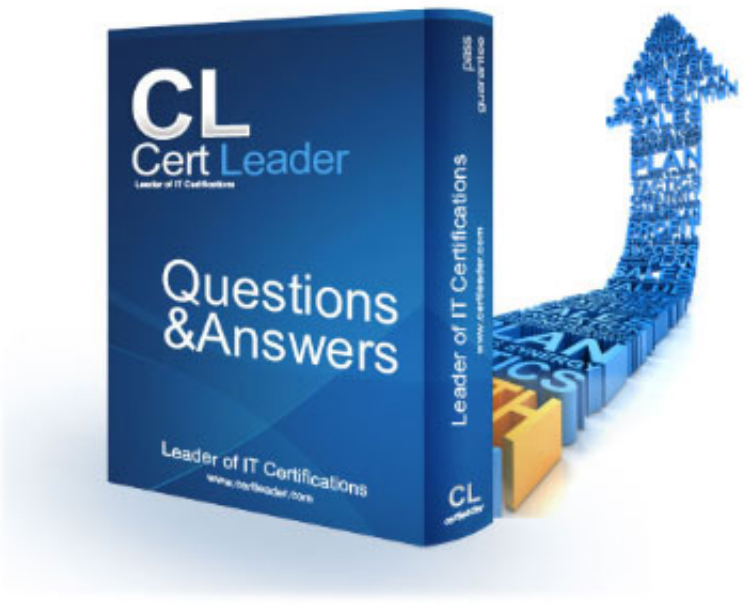
NSE4_FGT-7.0 Dumps

Fortinet NSE 4 - FortiOS 7.0

https://www.certleader.com/NSE4_FGT-7.0-dumps.html



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)
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 4
- (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 5
- (Exam Topic 1)
Which two configuration settings are synchronized when FortiGate devices are in an active-active HA cluster? (Choose two.)

A. FortiGuard web filter cache
B. FortiGate hostname
C. NTP
D. DNS

Answer: CD

NEW QUESTION 6
- (Exam Topic 1)
Which statement about video filtering on FortiGate is true?

A. Full SSL Inspection is not required.
B. It is available only on a proxy-based firewall policy.
C. It inspects video files hosted on file sharing services.
D. Video filtering FortiGuard categories are based on web filter FortiGuard categories.

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/190873/video-filtering

NEW QUESTION 7
- (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 8
- (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 9
- (Exam Topic 1)
Which CLI command allows administrators to troubleshoot Layer 2 issues, such as an IP address conflict?

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 1)
By default, FortiGate is configured to use HTTPS when performing live web filtering with FortiGuard servers. Which CLI command will cause FortiGate to use an unreliable protocol to communicate with FortiGuard
servers for live web filtering?

A. set fortiguard-anycast disable
B. set webfilter-force-off disable
C. set webfilter-cache disable
D. set protocol tcp

Answer: A

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=FD48294

NEW QUESTION 10
- (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 14
- (Exam Topic 1)
Refer to the exhibit.

An administrator is running a sniffer command as shown in the exhibit.
Which three pieces of information are included in the sniffer output? (Choose three.)

A. Interface name
B. Ethernet header
C. IP header
D. Application header
E. Packet payload

Answer: ACE

Explanation:
Reference: https://kb.fortinet.com/kb/documentLink.do?externalID=11186

NEW QUESTION 16
- (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 19
- (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 21
- (Exam Topic 2)
You have enabled logging on your FortiGate device for Event logs and all Security logs, and you have set up logging to use the FortiGate local disk.
What is the default behavior when the local disk is full?

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

Answer: C

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

NEW QUESTION 25
- (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 30
- (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 35
- (Exam Topic 2)
An administrator is running the following sniffer command:
Which three pieces of Information will be Included in me sniffer output? {Choose three.)

A. Interface name
B. Packet payload
C. Ethernet header
D. IP header
E. Application header

Answer: ABD

NEW QUESTION 39
- (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 43
- (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 45
- (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 47
- (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 49
- (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 53
- (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 54
- (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 58
- (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 62
- (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 67
- (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 72
- (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 73
- (Exam Topic 2)
Which statements are true regarding firewall policy NAT using the outgoing interface IP address with fixed port disabled? (Choose two.)

A. This is known as many-to-one NAT.
B. Source IP is translated to the outgoing interface IP.
C. Connections are tracked using source port and source MAC address.
D. Port address translation is not used.

Answer: BD

NEW QUESTION 75
- (Exam Topic 2)
Which downstream FortiGate VDOM is used to join the Security Fabric when split-task VDOM is enabled on all FortiGate devices?

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

Answer: A

NEW QUESTION 79
- (Exam Topic 2)
Which of the following statements is true regarding SSL VPN settings for an SSL VPN portal?

A. By default, FortiGate uses WINS servers to resolve names.
B. By default, the SSL VPN portal requires the installation of a client's certificate.
C. By default, split tunneling is enabled.
D. By default, the admin GUI and SSL VPN portal use the same HTTPS port.

Answer: D

NEW QUESTION 84
- (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 85
- (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 89
- (Exam Topic 2)
Which three authentication timeout types are availability for selection on FortiGate? (Choose three.)

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

Answer: ADE

Explanation:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD37221

NEW QUESTION 94
- (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 99
- (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 100
- (Exam Topic 2)
Which three statements are true regarding session-based authentication? (Choose three.)

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

Answer: ACD

NEW QUESTION 105
- (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 106
- (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 109
- (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 114
- (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 119
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your NSE4_FGT-7.0 Exam with Our Prep Materials Via below:

https://www.certleader.com/NSE4_FGT-7.0-dumps.html