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)
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 3
- (Exam Topic 1)
A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes.
* All traffic must be routed through the primary tunnel when both tunnels are up
* The secondary tunnel must be used only if the primary tunnel goes down
* In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover
Which two key configuration changes are needed on FortiGate to meet the design requirements? (Choose two,)

A. Configure a high distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.
B. Enable Dead Peer Detection.
C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
D. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.

Answer: BC

Explanation:

B - because the customer requires the tunnels to notify when a tunnel goes down. DPD is designed for that purpose. To send a packet over a firewall to determine a failover for the next tunnel after a specific amount of time of not receiving a response from its peer.
C - remember when it comes to choosing a route with regards to Administrative Distance. The route with the lowest distance for that particular route will be chosen. So, by configuring a lower routing distance on the primary tunnel, means that the primary tunnel will be chosen to route packets towards their destination.

NEW QUESTION 4
- (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 5
- (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 6
- (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 7
- (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 8
- (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 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)
Refer to the web filter raw logs.

Based on the raw logs shown in the exhibit, which statement is correct?

A. Social networking web filter category is configured with the action set to authenticate.
B. The action on firewall policy ID 1 is set to warning.
C. Access to the social networking web filter category was explicitly blocked to all users.
D. The name of the firewall policy is all_users_web.

Answer: A

NEW QUESTION 10
- (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 13
- (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 14
- (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 19
- (Exam Topic 1)
Which three statements about a flow-based antivirus profile are correct? (Choose three.)

A. IPS engine handles the process as a standalone.
B. FortiGate buffers the whole file but transmits to the client simultaneously.
C. If the virus is detected, the last packet is delivered to the client.
D. Optimized performance compared to proxy-based inspection.
E. Flow-based inspection uses a hybrid of scanning modes available in proxy-based inspection.

Answer: BDE

Explanation:
Reference: https://forum.fortinet.com/tm.aspx?m=192309

NEW QUESTION 23
- (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 28
- (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.

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 34
- (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 38
- (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 43
- (Exam Topic 1)
Refer to the exhibit.

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

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

Answer: A

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

NEW QUESTION 46
- (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 47
- (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)
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 51
- (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 55
- (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 58
- (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 62
- (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 64
- (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 67
- (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 70
- (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 72
- (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 75
- (Exam Topic 2)
Which two statements are correct regarding FortiGate FSSO agentless polling mode? (Choose two.)

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

Answer: CD

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

NEW QUESTION 79
- (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 84
- (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 89
- (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 94
- (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 98
- (Exam Topic 2)
When a firewall policy is created, which attribute is added to the policy to support recording logs to a FortiAnalyzer or a FortiManager and improves functionality when a FortiGate is integrated with these devices?

A. Log ID
B. Universally Unique Identifier
C. Policy ID
D. Sequence ID

Answer: B

Explanation:
Reference: https://docs.fortinet.com/document/fortigate/6.0.0/handbook/554066/firewall-policies

NEW QUESTION 99

- (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 100
- (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 104
- (Exam Topic 2)
Which feature in the Security Fabric takes one or more actions based on event triggers?

A. Fabric Connectors
B. Automation Stitches
C. Security Rating
D. Logical Topology

Answer: B

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

NEW QUESTION 108
- (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 113
- (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 116
- (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 117
- (Exam Topic 2)
Which two statements about IPsec authentication on FortiGate are correct? (Choose two.)

A. For a stronger authentication, you can also enable extended authentication (XAuth) to request the remote peer to provide a username and password
B. FortiGate supports pre-shared key and signature as authentication methods.
C. Enabling XAuth results in a faster authentication because fewer packets are exchanged.
D. A certificate is not required on the remote peer when you set the signature as the authentication method.

Answer: AB

Explanation:
Reference:
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/913287/ipsec-vpn-authenticating-aremote-fortigate

NEW QUESTION 120
- (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 123
- (Exam Topic 2)
Refer to the exhibit.

The exhibit contains a network diagram, central SNAT policy, and IP pool configuration. The WAN (port1) interface has the IP address 10.200.1.1/24.
The LAN (port3) interface has the IP address 10.0.1.254/24.
A firewall policy is configured to allow to destinations from LAN (port3) to WAN (port1). Central NAT is enabled, so NAT settings from matching Central SNAT policies will be applied.
Which IP address will be used to source NAT the traffic, if the user on Local-Client (10.0.1.10) pings the IP address of Remote-FortiGate (10.200.3.1)?

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

Answer: D

NEW QUESTION 127
- (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 130
- (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 132
- (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 136
- (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 137
- (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 140
- (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 144
- (Exam Topic 2)
Examine the network diagram shown in the exhibit, then answer the following question:

Which one of the following routes is the best candidate route for FGT1 to route traffic from the Workstation to the Web server?

A. 172.16.0.0/16 [50/0] via 10.4.200.2, port2 [5/0]
B. 0.0.0.0/0 [20/0] via 10.4.200.2, port2
C. 10.4.200.0/30 is directly connected, port2
D. 172.16.32.0/24 is directly connected, port1

Answer: D

NEW QUESTION 146
- (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 151
- (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 154
- (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 157
- (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 160
- (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 162
- (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 166
- (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 168
- (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 171
- (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 175
- (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 176
- (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 179
- (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 183
- (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 184
- (Exam Topic 2)
Which of the following statements about backing up logs from the CLI and downloading logs from the GUI are true? (Choose two.)

A. Log downloads from the GUI are limited to the current filter view
B. Log backups from the CLI cannot be restored to another FortiGate.
C. Log backups from the CLI can be configured to upload to FTP as a scheduled time
D. Log downloads from the GUI are stored as LZ4 compressed files.

Answer: AB

NEW QUESTION 187
- (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 192
- (Exam Topic 2)
Which certificate value can FortiGate use to determine the relationship between the issuer and the certificate?

A. Subject Key Identifier value
B. SMMIE Capabilities value
C. Subject value
D. Subject Alternative Name value

Answer: A

NEW QUESTION 195

- (Exam Topic 2)
Which statement regarding the firewall policy authentication timeout is true?

A. It is an idle timeou
B. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source IP.
C. It is a hard timeou
D. The FortiGate removes the temporary policy for a user’s source IP address after this timer has expired.
E. It is an idle timeou
F. The FortiGate considers a user to be “idle” if it does not see any packets coming from the user’s source MAC.
G. It is a hard timeou
H. The FortiGate removes the temporary policy for a user’s source MAC address after this timer has expired.

Answer: A

NEW QUESTION 200
- (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 202
- (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 206
- (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 208
- (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 209
- (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 212
- (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 216
- (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 219
- (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 222
- (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 223
- (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 227
- (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 232
- (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 235
- (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 237
- (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 239
- (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 242
- (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 243
.....

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