Exam Questions NSE4

Fortinet Network Security Expert 4 Written Exam (400)

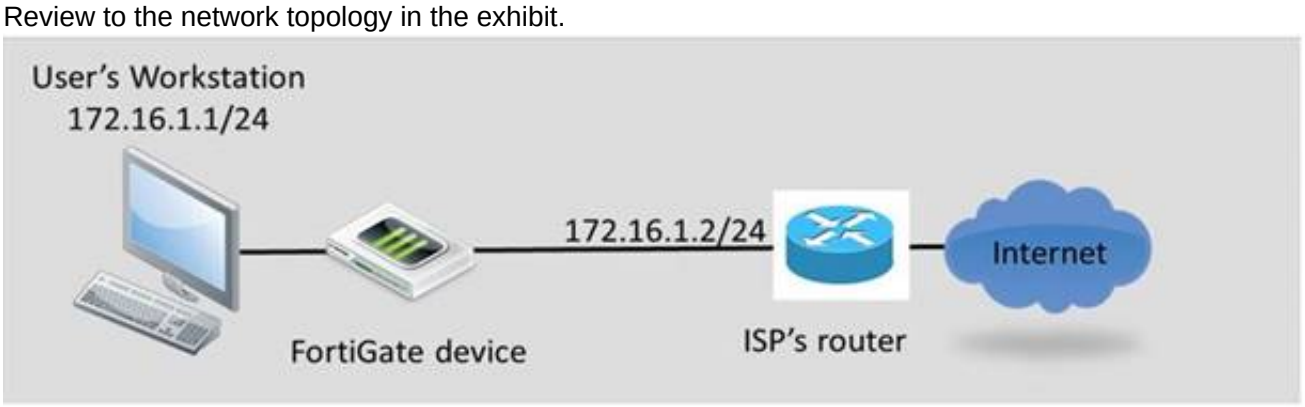
https://www.2passeasy.com/dumps/NSE4/

NEW QUESTION 1
A FortiGate administrator with the super_admin profile configures a virtual domain (VDOM) for a new customer. After creating the VDOM, the administrator is unable to reassign the dmz interface to the new VDOM as the option is greyed out in the GUI in the management VDOM.
What would be a possible cause for this problem?

A. The administrator does not have the proper permissions the dmz interface.
B. The dmz interface is referenced in the configuration of another VDOM.
C. Non-management VDOMs cannot reference physical interfaces
D. The dmz interface is in PPPoE or DHCP mode.

Answer: B

NEW QUESTION 2
Review to the network topology in the exhibit.



The workstation, 172.16.1.1/24, connects to port2 of the FortiGate device, and the ISP router, 172.16.1.2, connects to port1. Without changing IP addressing, which configuration changes are required to properly forward users traffic to the Internet? (Choose two)

A. At least one firewall policy from port2 to port1 to allow outgoing traffic.
B. A default route configured in the FortiGuard devices pointing to the ISP's router.
C. Static or dynamic IP addresses in both ForitGate interfaces port1 and port2.
D. The FortiGate devices configured in transparent mode.

Answer: AD

NEW QUESTION 3
Which best describes the authentication timeout?

A. How long FortiGate waits for the user to enter his or her credentials.
B. How long a user is allowed to send and receive traffic before he or she must authenticate again.
C. How long an authenticated user can be idle (without sending traffic) before they must authenticate again.
D. How long a user-authenticated session can exist without having to authenticate again.

Answer: C

NEW QUESTION 4
FSSO provides a single sign on solution to authenticate users transparently to a FortiGate unit using credentials stored in Windows active directory.
Which of the following statements are correct regarding FSSO in a Windows domain environment when DC-agent mode is used? (Choose two.)

A. An FSSO collector agent must be installed on every domain controller.
B. An FSSO domain controller agent must be installed on every domain controller.
C. The FSSO domain controller agent will regularly update user logon information on the FortiGate unit.
D. The FSSO collector agent will receive user logon information from the domain controller agent and will send it to the FortiGate unit.

Answer: BD

NEW QUESTION 5
Which two statements are true regarding firewall policy disclaimers? (Choose two.)

A. They cannot be used in combination with user authentication.
B. They can only be applied to wireless interfaces.
C. Users must accept the disclaimer to continue.
D. The disclaimer page is customizable.

Answer: CD

NEW QUESTION 6
With FSSO DC-agent mode, a domain user could authenticate either against the domain controller running the collector agent and domain controller agent, or a domain controller running only the domain controller agent.
If you attempt to authenticate with a domain controller running only the domain controller agent, which statements are correct? (Choose two.)

A. The login event is sent to a collector agent.
B. The FortiGate receives the user information directly from the receiving domain controller agent of the secondary domain controller.
C. The domain collector agent may perform a DNS lookup for the authenticated client's IP address.
D. The user cannot be authenticated with the FortiGate in this manner because each domain controller agent requires a dedicated collector agent.

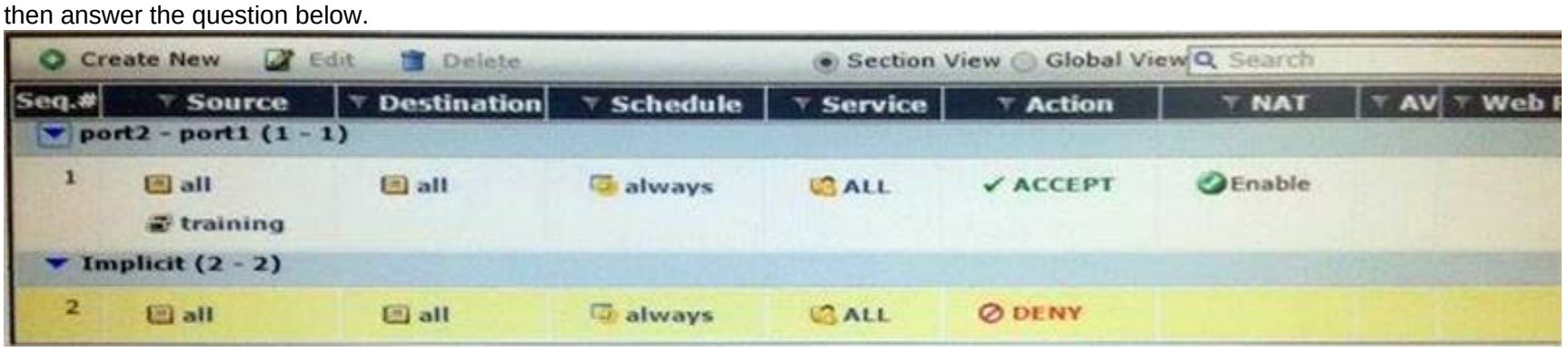
Answer: AC

NEW QUESTION 7
Which of the following fields contained in the IP/TCP/UDP headers can be used to make a routing decision when using policy-based routing? (Choose three)

A. Source IP address.
B. TCP flags
C. Source TCP/UDP ports
D. Type of service.
E. Checksum

Answer: ACD

NEW QUESTION 8
The FortiGate port1 is connected to the Internet. The FortiGate port2 is connected to the internal network. Examine the firewall configuration shown in the exhibit; then answer the question below.



Based on the firewall configuration illustrated in the exhibit, which statement is correct?

A. A user that has not authenticated can access the Internet using any protocol that does not trigger an authentication challenge.
B. A user that has not authenticated can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP.
C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access all Internet services.
D. DNS Internet access is always allowed, even for users that have not authenticated.

Answer: D

NEW QUESTION 9
Which of the following statements is true regarding the use of a PAC file to configure the web proxy settings in an Internet browser? (Choose two.)

A. More than one proxy is supported.
B. Can contain a list of destinations that will be exempt from the use of any proxy.
C. Can contain a list of URLs that will be exempted from the FortiGate web filtering inspection.
D. Can contain a list of users that will be exempted from the use of any proxy.

Answer: BC

NEW QUESTION 10
Which of the following statements is true regarding a FortiGate device operating in transparent mode? (Choose three.)

A. It acts as a layer 2 bridge
B. It acts as a layer 3 router
C. It forwards frames using the destination MAC address.
D. It forwards packets using the destination IP address.
E. It can perform content inspection (antivirus, web filtering, etc)

Answer: ACE

NEW QUESTION 10
Which is true about incoming and outgoing interfaces in firewall policies?

A. A physical interface may not be used.
B. A zone may not be used.
C. Multiple interfaces may not be used for both incoming and outgoing.
D. Source and destination interfaces are mandatory.

Answer: D

NEW QUESTION 15
Which of the following statements are correct regarding a master HA unit? (Choose two)

A. There should be only one master unit is each HA virtual cluster.
B. The Master synchronizes cluster configuration with slaves.
C. Only the master has a reserved management HA interface.
D. Heartbeat interfaces are not required on a master unit.

Answer: AB

NEW QUESTION 16
For data leak prevention, which statement describes the difference between the block and quarantine actions?

A. A block action prevents the transactio
B. A quarantine action blocks all future transactions, regardless of the protocol.
C. A block action prevents the transactio
D. A quarantine action archives the data.
E. A block action has a finite duratio
F. A quarantine action must be removed by an administrator.
G. A block action is used for known user
H. A quarantine action is used for unknown users.

Answer: A

NEW QUESTION 17
Examine the output below from the diagnose sys top command:

```
# diagnose sys top 1
Run time: 11 days, 3 hours and 29 minutes
OU,   ON,   1S,   99I;   971T,  528F,  160 KF
sshd          123          S      1.9     1.2
ipsendjine    61           S <    0.0     5.2
miglogd       45           S      0.0     4.9
pyfcgid       75           S      0.0     4.5
pyfcgid       73           S      0.0     3.9
```

Which statements are true regarding the output above (Choose two.)

A. The sshd process is the one consuming most CPU.
B. The sshd process is using 123 pages of memory.
C. The command diagnose sys kill miglogd will restart the miglogd process.
D. All the processes listed are in sleeping state.

Answer: AD

NEW QUESTION 19
Which of the following authentication methods can be used for SSL VPN authentication? (Choose three.)

A. Remote Password Authentication (RADIUS, LDAP)
B. Two-Factor Authentication
C. Local Password Authentication
D. FSSO
E. RSSO

Answer: ABC

NEW QUESTION 21
What log type would indicate whether a VPN is going up or down?

A. Event log
B. Security log
C. Forward log
D. Syslog

Answer: A

NEW QUESTION 23
Which antivirus inspection mode must be used to scan SMTP, FTP, POP3 and SMB protocols?

A. Proxy-based.
B. DNS-based.
C. Flow-based.
D. Man-in-the-middle.

Answer: C

NEW QUESTION 28
Where are most of the security events logged?

A. Security log
B. Forward Traffic log
C. Event log
D. Alert log
E. Alert Monitoring Console

Answer: C

NEW QUESTION 31
Which statement is correct concerning an IPsec VPN with the remote gateway setting configured as 'Dynamic DNS'?

A. The FortiGate will accept IPsec VPN connection from any IP address.
B. The FQDN resolution of the local FortiGate IP address where the VPN is terminated must be provided by a dynamic DNS provider.
C. The FortiGate will Accept IPsec VPN connections only from IP addresses included on a dynamic DNS access list.
D. The remote gateway IP address can change dynamically.

Answer: D

NEW QUESTION 34
When an administrator attempts to manage FortiGate from an IP address that is not a trusted host, what happens?

A. FortiGate will still subject that person's traffic to firewall policies; it will not bypass them.
B. FortiGate will drop the packets and not respond.
C. FortiGate responds with a block message, indicating that it will not allow that person to log in.
D. FortiGate responds only if the administrator uses a secure protoco
E. Otherwise, it does not respond

Answer: B

NEW QUESTION 36
Which is not a FortiGate feature?

A. Database auditing
B. Intrusion prevention
C. Web filtering
D. Application control

Answer: A

NEW QUESTION 40
Examine the following spanning tree configuration on a FortiGate in transparent mode:
config system interface edit <interface name> set stp-forward enable end
Which statement is correct for the above configuration?

A. The FortiGate participates in spanning tree.
B. The FortiGate device forwards received spanning tree messages.
C. Ethernet layer-2 loops are likely to occur.
D. The FortiGate generates spanning tree BPDU frames.

Answer: B

NEW QUESTION 42
Which of the following actions can be used to back up the keys and digital certificates in a FortiGate device? (Choose two.)

A. Taking a full backup of the FortiGate configuration
B. Uploading a PKCS#10 file to a USB drive
C. Manually uploading the certificate information to a Certificate authority (CA)
D. Uploading a PKCS#12 file to a TFTP server

Answer: AD

NEW QUESTION 46
Which TCP states does the global setting ‘tcp-half-open-timer’ applies to? (Choose two.)

A. SYN SENT
B. SYN & SYN/ACK
C. FIN WAIT
D. TIME WAIT

Answer: AD

NEW QUESTION 50
A backup file begins with this line:
#config-version=FGVM64-5.02-FW-build589-140613:opmode=0:vdom=0:user=admin
#conf_file_ver=3881503152630288414 #buildno=0589 #global_vdom=1
Can you restore it to a FortiWiFi 60D?

A. Yes
B. Yes, but only if you replace the "#conf_file_ver" line so that it contains the serial number of that specific FortiWiFi 60D.
C. Yes, but only if it is running the same version of FortiOS, or a newer compatible version.
D. No

Answer: D

NEW QUESTION 51
Which is the following statement are true regarding application control? (choose two)

A. Application control is based on TCP destination port numbers.
B. Application control is proxy based.
C. Encrypted traffic can be identified by application control.
D. Traffic Shaping can be applied to the detected application traffic.

Answer: CD

NEW QUESTION 56
Which statement best describes what SSL VPN Client Integrity Check does?

A. Blocks SSL VPN connection attempts from users that has been blacklisted.
B. Detects the Windows client security applications running in the SSL VPN client's PCs.
C. Validates the SSL VPN user credential.
D. Verifies which SSL VPN portal must be presented to each SSL VPN user.
E. Verifies that the latest SSL VPN client is installed in the client's PC.

Answer: B

NEW QUESTION 60
Which best describe the mechanism of a TCP SYN flood?

A. The attacker keeps open many connections with slow data transmission so that other clients cannot start new connections.
B. The attacker sends a packet designed to "sync" with the FortiGate.
C. The attacker sends a specially crafted malformed packet, intended to crash the target by exploiting its parser.
D. The attacker starts many connections, but never acknowledges to fully form them.

Answer: D

NEW QUESTION 63
A FortiGate device is configure to perform an AV & IPS scheduled update every hour.

```
Virus Definitions
---------
Version: 21.00487
Contract Expiry Date: Tue Apr 29 00:00:00 2014
Last Updated using scheduled update on Mon Jan
20 01:05:33 2014
Last Update Attempt: Mon Jan 20 10:08:56 2014
Result: Updates Installed
```

```
FG100D3G12800939 # exe time
current time is: 10:35:35
last ntp sync:Mon Jan 20 09:51:59 2014
```

Given the information in the exhibit, when will the next update happen?

A. 01:00
B. 02:05
C. 11:00
D. 11:08

Answer: D

NEW QUESTION 65
Which of the following statements describe some of the differences between symmetric and asymmetric cryptography? (Choose two.)

A. In symmetric cryptography, the keys are publicly availabl
B. In asymmetric cryptography, the keys must be kept secret.
C. Asymmetric cryptography can encrypt data faster than symmetric cryptography
D. Symmetric cryptography uses one pre-shared ke
E. Asymmetric cryptography uses a pair or keys
F. Asymmetric keys can be sent to the remote peer via digital certificate
G. Symmetric keys cannot

Answer: CD

NEW QUESTION 68

An administrator has configured a route-based site-to-site IPsec VPN. Which statement is correct regarding this IPsec VPN configuration?

A. The IPsec firewall policies must be placed at the top of the list.
B. This VPN cannot be used as a part of a hub and spoke topology.
C. Routes are automatically created based on the quick mode selectors.
D. A virtual IPsec interface is automatically created after the Phase 1 configuration is completed.

Answer: D

NEW QUESTION 71
An Internet browser is using the WPAD DNS method to discover the PAC file's URL. The DNS server replies to the browser's request with the IP address 10.100.1.10. Which URL will the browser use to download the PAC file?

A. http://10.100.1.10/proxy.pac
B. https://10.100.1.10/
C. http://10.100.1.10/wpad.dat
D. https://10.100.1.10/proxy.pac

Answer: C

NEW QUESTION 73
Which statements regarding banned words are correct? (Choose two.)

A. Content is automatically blocked if a single instance of a banned word appears.
B. The FortiGate updates banned words on a periodic basis.
C. The FortiGate can scan web pages and email messages for instances of banned words.
D. Banned words can be expressed as simple text, wildcards and regular expressions.

Answer: CD

NEW QUESTION 78
Which operating system vulnerability can you protect when selecting signatures to include in an IPS sensor? (choose three)

A. Irix
B. QNIX
C. Linux
D. Mac OS
E. BSD

Answer: CDE

NEW QUESTION 82
Which is true of FortiGate's session table?

A. NAT/PAT is shown in the central NAT table, not the session table.
B. It shows TCP connection states.
C. It shows IP, SSL, and HTTP sessions.
D. It does not show UDP or ICMP connection state codes, because those protocols are connectionless.

Answer: B

NEW QUESTION 87
Examine the following output from the diagnose sys session list command:

```
session info: proto=6 proto_state=65 duration=3 expire=9 timeout=3600 flags=00000000
sockflag=00000000 sockport=443 av_idx=9 use=5

origin-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps

reply-shaper=guarantee-100kbps prio=2 guarantee 12800Bps max 134217728Bps traffic 13895Bps

state=redir local may_dirty ndr npu nlb os rs

statistic(bytes/packets/allow_err): org=864/8/1 reply=2384/7/1 tuples=3

orgin->sink: org pre->post, reply pre->post dev=7->6/6->7 gwy=172.17.87.3/10.1.10.1

hook=post dir=org act=snat 192.168.1.110:57999->74.201.86.29:443(172.17.87.16:57999)

hook=pre dir=reply act=dnat 74.201.86.29:443->172.17.87.16:57999(192.168.1.110:57999)

hook=post dir=reply act=noop 74.201.86.29:443->192.168.1.110:57999(0.0.0.0:0)

misc=0 policy_id=1 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0

npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0/0
```

Which statements are true regarding the session above? (Choose two.)

A. Session Time-To-Live (TTL) was configured to 9 seconds.
B. FortiGate is doing NAT of both the source and destination IP address on all packets coming from the 192.168.1.110 address.
C. The IP address 192.168.1.110 is being translated to 172.17.87.16.
D. The FortiGate is not translating the TCP port numbers of the packets in this session.

Answer: CD

NEW QUESTION 89
Which of the following statements are correct concerning IKE mode config? (Choose two)

A. It can dynamically assign IP addresses to IPsec VPN clients.
B. It can dynamically assign DNS settings to IPsec VPN clients.
C. It uses the ESP protocol.
D. It can be enabled in the phase 2 configuration.

Answer: AB

NEW QUESTION 91
In a FSSO agent mode solution, how does the FSSO collector agent learn each IP address?

A. The DC agents get each user IP address from the event logs and forward that information to the collector agent
B. The collector agent does not know, and does not need, each user IP addres
C. Only workstation names are known by the collector agent.
D. The collector agent frequently polls the AD domain controllers to get each user IP address.
E. The DC agent learns the workstation name from the event logs and DNS is then used to translate those names to the respective IP addresses.

Answer: D

NEW QUESTION 92
Which statement is in advantage of using a hub and spoke IPsec VPN configuration instead of a fully-meshed set of IPsec tunnels?

A. Using a hub and spoke topology provides full redundancy.
B. Using a hub and spoke topology requires fewer tunnels.
C. Using a hub and spoke topology uses stronger encryption protocols.
D. Using a hub and spoke topology requires more routes.

Answer: B

NEW QUESTION 97
Files that are larger than the oversized limit are subjected to which Antivirus check?

A. Grayware
B. Virus
C. Sandbox
D. Heuristic

Answer: C

NEW QUESTION 100
A static route is configured for a FortiGate unit from the CLI using the following commands:
config router static edit 1
set device “wan1” set distance 20
set gateway 192.168.100.1 next
end
Which of the following conditions are required for this static default route to be displayed in the FortiGate unit's routing table? (Choose two.)

A. The administrative status of the wan1 interface is displayed as down.
B. The link status of the wan1 interface is displayed as up.
C. All other default routers should have a lower distance.
D. The wan1 interface address and gateway address are on the same subnet.

Answer: BD

NEW QUESTION 104
Which statements are correct regarding application control? (Choose two.)

A. It is based on the IPS engine.
B. It is based on the AV engine.
C. It can be applied to SSL encrypted traffic.
D. It cannot be applied to SSL encrypted traffic.

Answer: AC

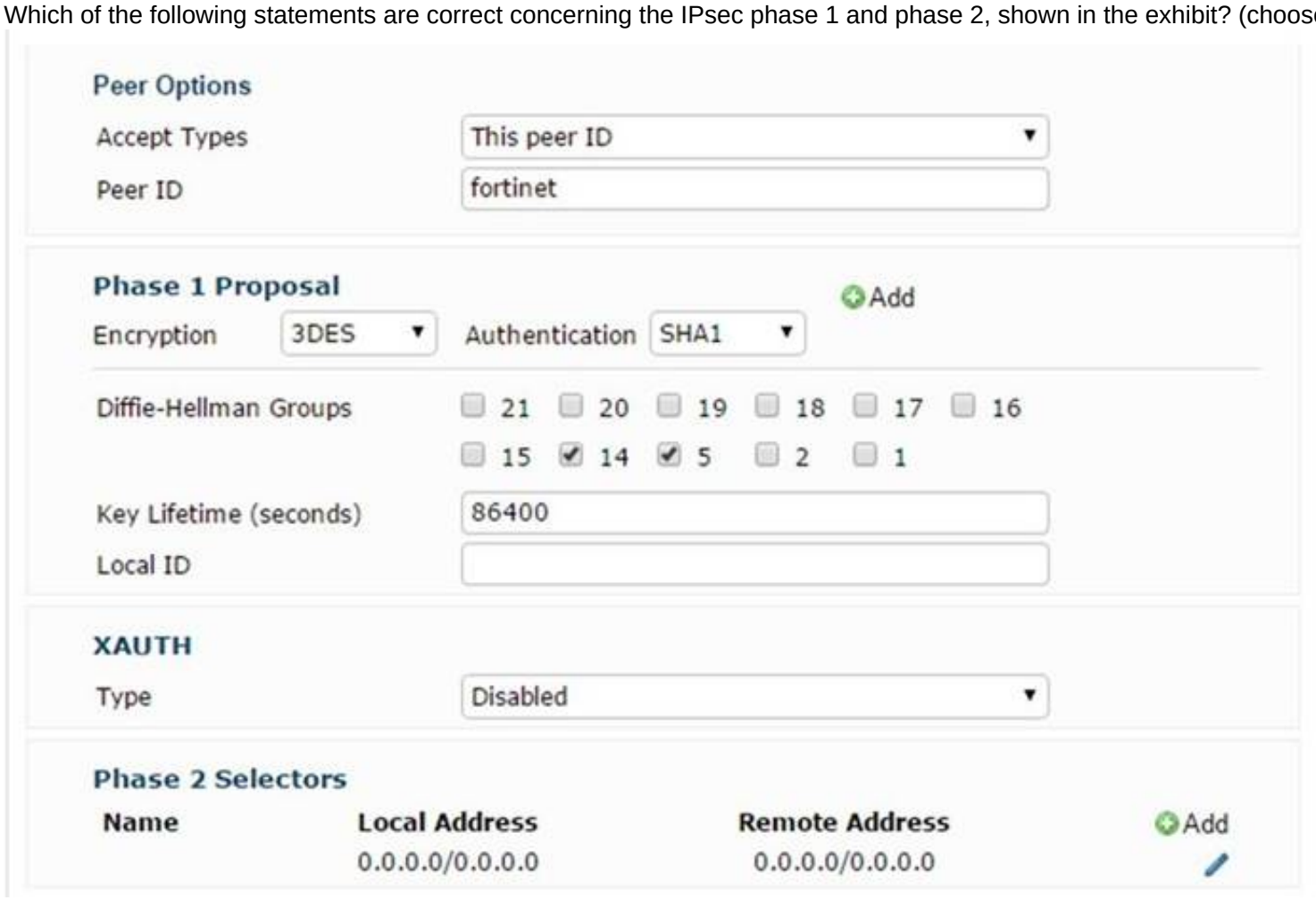
NEW QUESTION 108
Which does FortiToken use as input when generating a token code? (Choose two.)

A. User password
B. Time
C. User name
D. Seed

Answer: AD

Explanation:
The token passcode is generated using a combination of the time and a secret key which is known only by the token and the FortiAuthenticator device. The token password changes at regular time intervals, and the FortiAuthenticator unit is able to validate the entered passcode using the time and the secret seed information for that token.

NEW QUESTION 112
Which of the following statements are correct concerning the IPsec phase 1 and phase 2, shown in the exhibit? (choose two)



A. The quick mode selector in the remote site must also be 0.0.0.0/0 for the source and destination addresses.
B. Only remote peers with the peer ID 'fortinet' will be able to establish a VPN.
C. The FortiGate device will automatically add a static route to the source quick mode selector address received from each remote VPN peer.
D. The configuration will work only to establish FortiClient-to-FortiGate tunnel
E. A FortiGate tunnel requires a different configuration.

Answer: CD

NEW QUESTION 116
You are the administrator in charge of a FortiGate acting as an IPsec VPN gateway using routebased mode. Users from either side must be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate already has a default route.
Which two configuration steps are required to achieve these objectives? (Choose two.)

A. Create one firewall policy.
B. Create two firewall policies.
C. Add a route to the remote subnet.
D. Add two IPsec phases 2.

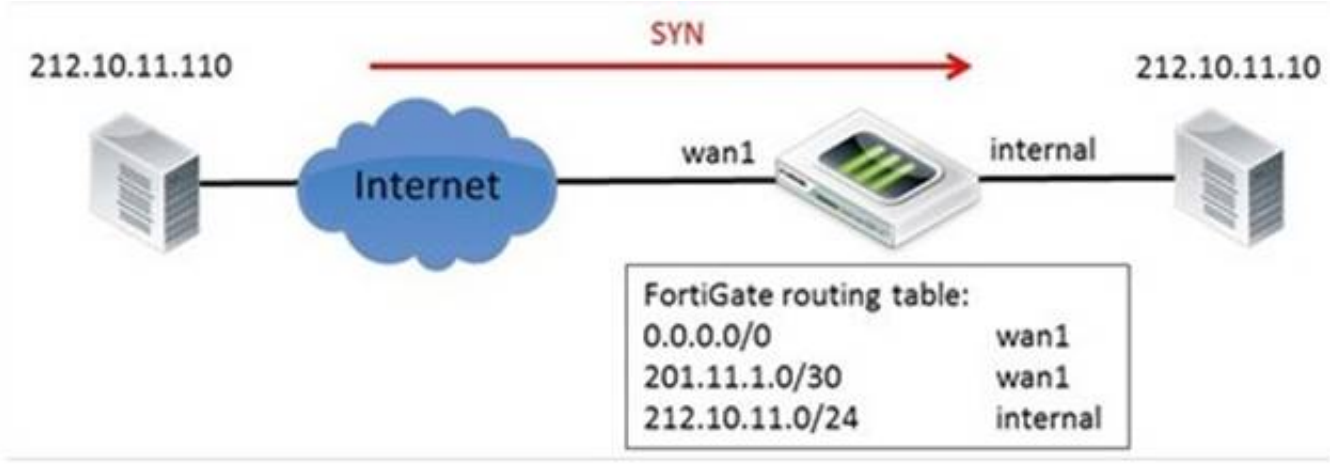
Answer: BC

NEW QUESTION 120
Which of the following actions that can be taken by the Data Leak Prevention scanning? (Choose three.)

A. Block
B. Reject
C. Tag
D. Log only
E. Quarantine IP address

Answer: ADE

NEW QUESTION 123
Examine the network topology diagram in the exhibit; the workstation with the IP address 212.10.11.110 sends a TCP SYN packet to the workstation with the IP address 212.10.11.20.



Which of the following sentences best describes the result of the reverse path forwarding (RFP) check executed by the FortiGate on the SYN packets? (Choose two).

A. Packets is allowed if RPF is configured as loose.
B. Packets is allowed if RPF is configured as strict.
C. Packets is blocked if RPF is configured as loose.
D. Packets is blocked if RPF is configured as strict.

Answer: AD

NEW QUESTION 127
Which is NOT true about the settings for an IP pool type port block allocation?

A. A Block Size defines the number of connections.
B. Blocks Per User defines the number of connection blocks for each user.
C. An Internal IP Range defines the IP addresses permitted to use the pool.
D. An External IP Range defines the IP addresses in the pool.

Answer: B

NEW QUESTION 130
Regarding the use of web-only mode SSL VPN, which statement is correct?

A. It support SSL version 3 only.
B. It requires a Fortinet-supplied plug-in on the web client.
C. It requires the user to have a web browser that suppports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client.

Answer: C

NEW QUESTION 132
Which of the following network protocols can be inspected by the Data Leak Prevention scanning? (Choose three.)

A. SMTP
B. HTTP-POST
C. AIM
D. MAPI
E. ICQ

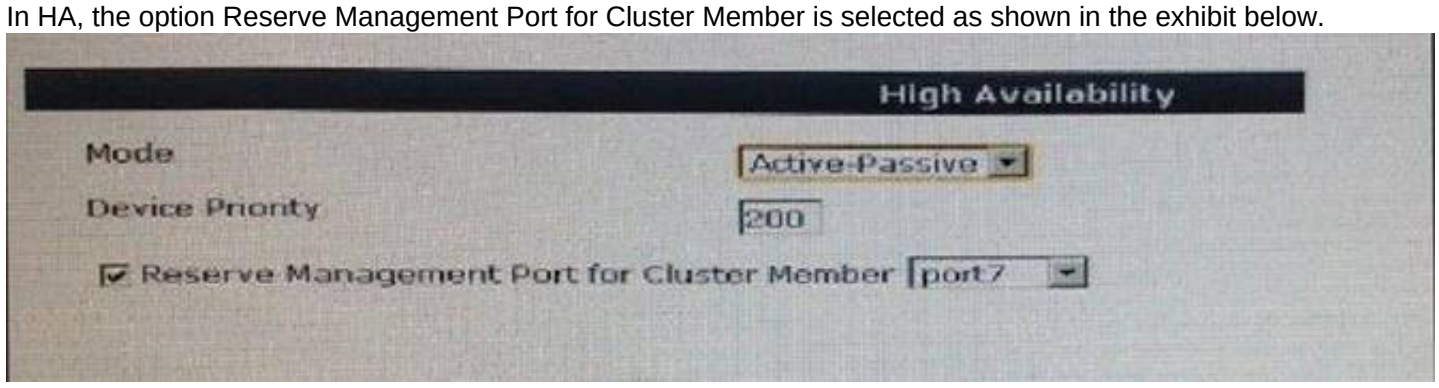
Answer: ABD

NEW QUESTION 133
Which web filtering inspection mode inspects DNS traffic?

A. DNS-based.
B. FQDN-based.
C. Flow-based.
D. URL-based.

Answer: A

NEW QUESTION 137
In HA, the option Reserve Management Port for Cluster Member is selected as shown in the exhibit below.



Which statements are correct regarding this setting? (Choose two.)

A. Interface settings on port7 will not be synchronized with other cluster members.
B. The IP address assigned to this interface must not overlap with the IP address subnet assigned to another interface.
C. When connecting to port7 you always connect to the master device.
D. A gateway address may be configured for port7.

Answer: AD

NEW QUESTION 139
Two FortiGate units with NP6 processors form an active-active cluster. The cluster is doing security profile (UTM) inspection over all the user traffic.
What statements are true regarding the sessions that the master unit is offloading to the slave unit for inspection? (Choose two.)

A. They are accelerated by hardware in the master unit.
B. They are not accelerated by hardware in the master unit.
C. They are accelerated by hardware in the slave unit.
D. They are not accelerated by hardware in the slave unit.

Answer: AD

NEW QUESTION 140
Which of the following are operating mode supported in FortiGate devices? (Choose two)

A. Proxy
B. Transparent
C. NAT/route
D. Offline inspection

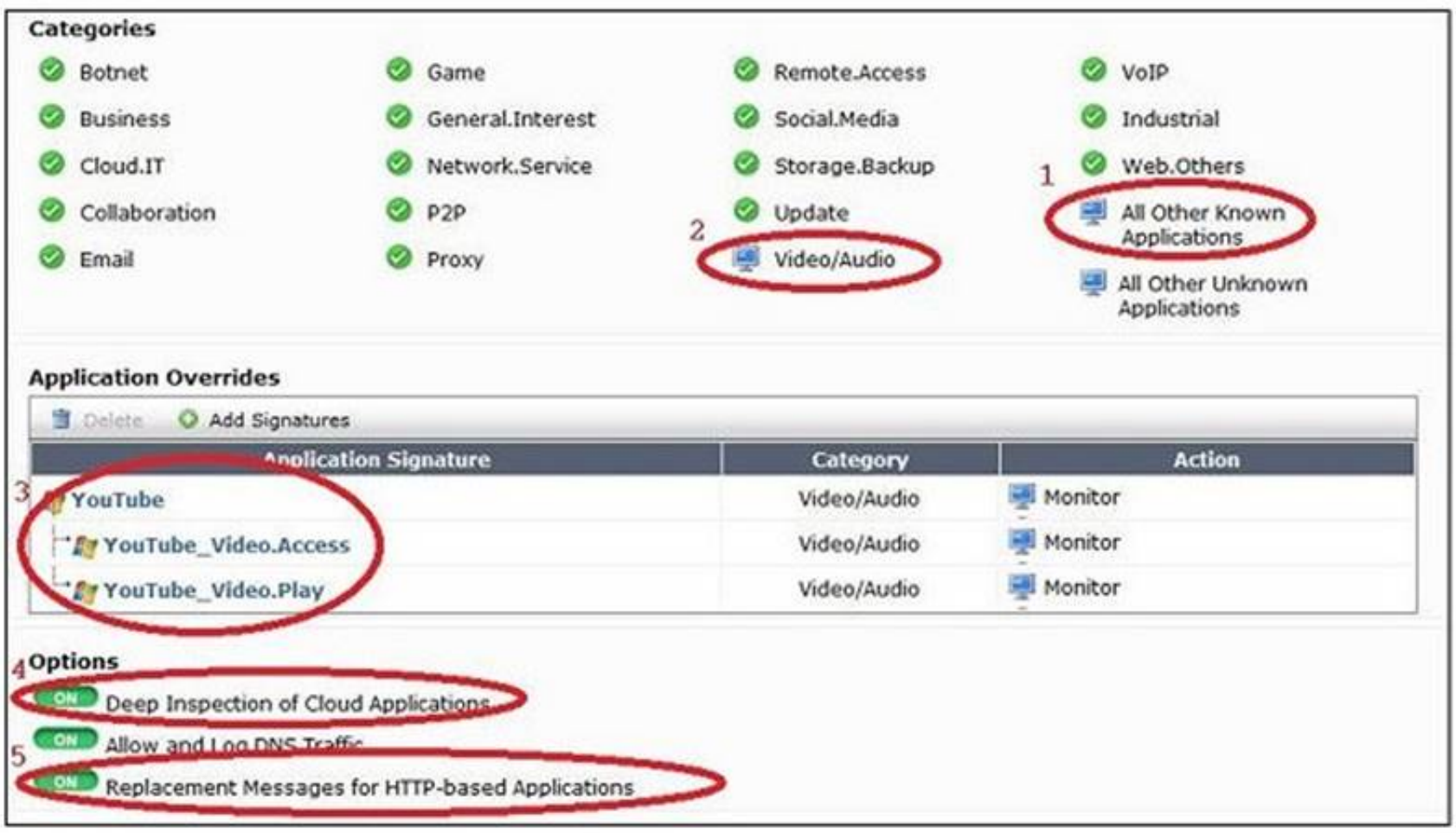
Answer: BC

NEW QUESTION 144
Which authentication scheme is not supported by the RADIUS implementation on FortiGate?

A. CHAP
B. MSCHAP2
C. PAP
D. FSSO

Answer: D

NEW QUESTION 149
The exhibit is a screen shot of an Application Control profile.



Different settings are circled and numbered. Select the number identifying the setting which will provide additional information about YouTube access, such as the name of the video watched.

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: D

NEW QUESTION 151
In a high availability cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a slave unit?

A. Client - > slave FortiGate - > master FortiGate - > web server.
B. Client - > slave FortiGate - > web server.
C. Client - > master FortiGate - > slave FortiGate - > master FortiGate - >web server.
D. Client - > master FortiGate - >slave FortiGate - > web server.

Answer: D

NEW QUESTION 156
The exhibit shows a FortiGate routing table.

```
# get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default
O*E2   0.0.0.0/0 [110/10] via 192.168.11.254, wan1, 01:29:24
C      172.16.78.0/24 is directly connected, wan2
O      192.168.1.0/24 [110/200] via 192.168.11.59, internal, 01:30:28
C      192.168.3.0/24 is directly connected, dmz
C      192.168.11.0/24 is directly connected, internal
```

Which of the following statements are correct?(Choose two)

A. There is only one active default route.
B. The distance values for the route to 192.168.1.0/24 is 200
C. An IP address in the subnet 172.16.78.0/24 has been assigned to the dmz interface.
D. The FortiGate will route the traffic to 172.17.1.2 to next hop with the IP address 192.168.11.254

Answer: AD

NEW QUESTION 157
Which statements correctly describe transparent mode operation? (Choose three.)

A. The FortiGate acts as transparent bridge and forwards traffic at Layer-2.
B. Ethernet packets are forwarded based on destination MAC addresses, NOT IP addresses.
C. The transparent FortiGate is clearly visible to network hosts in an IP trace route.
D. Permits inline traffic inspection and firewalling without changing the IP scheme of the network.
E. All interfaces of the transparent mode FortiGate device most be on different IP subnets.

Answer: ABD

NEW QUESTION 161
Which of the following statements are true about IPsec VPNs? (Choose three.)

A. IPsec increases overhead and bandwidth.
B. IPsec operates at the layer 2 of the OSI model.
C. End-user's network applications must be properly pre-configured to send traffic across the IPsec VPN.
D. IPsec protects upper layer protocols.
E. IPsec operates at the layer 3 of the OSI model.

Answer: ADE

NEW QUESTION 166
Review the IKE debug output for IPsec shown in the exhibit below.

```
STUDENT # ike 0: comes 10.200.3.1:500->10.200.1.1:500,ifindex=2....
ike 0: IKEv1 exchange=Informational id=9e2606ac7ae83d7a/612da78d3ab3f945:15b10705 len=92
ike 0: in 9E2606AC7AE83D7A612DA78D3AB3F945081005011581070500000005C26E2A7EC8461AC15E9BBC705B6C1F667A41957AED11FB7003C07A1
07BD934DD36E1A2C74348E38FD6B39146C618525C6EC51E2F26885B6BB8E035F52B4
ike 0:Remote_1:10: dec 9E2606AC7AE83D7A612DA78D3AB3F945081005011581070500000005C08000018E281874EECF170EB5222B6A4E3A027C71
C0000000200000000101108D289E2606AC7AE83D7A612DA78D3AB3F9450000009C17511ED6EE549507
ike 0:Remote_1:10: notify msg received: R-U-THERE
ike 0:Remote_1:10: enc 9E2606AC7AE83D7A612DA78D3AB3F9450810050173 4C5CDF0000005408000D181CD47F014CBEF1B0EC8DA915F3B18AEB0
A0000000200000000101108D299E2606AC7AE83D7A612DA78D3AB3F9450000009C
ike 0:Remote_1:10: out 9E2606AC7AE83D7A612DA78D3AB3F9450810050173 4C5CDF0000005CB3CC43106 5A1737144B02F1AACE79C1BE712B84255
BB84E5FA7A967FE99C7B731057FF33728BB42AA983E79C919DA9B64EBCE087EF0A02666C1FBD2C62F
ike 0:Remote_1:10: sent IKE msg (R-U-THERE-ACK): 10.200.1.1:500->10.200.3.1:500, len=92, id=9e2606ac7ae83d7a/612da78d3ab3
734c5cdf
ike 0:Remote_1: link is idle 2 10.200.1.1->10.200.3.1:500 dpd=1 seqno=34
```

Which statements is correct regarding this output?

A. The output is a phase 1 negotiation.
B. The output is a phase 2 negotiation.
C. The output captures the dead peer detection messages.
D. The output captures the dead gateway detection packets.

Answer: C

NEW QUESTION 171
A FortiGate devices has two VDOMs in NAT/route mode. Which of the following solutions can be implemented by a network administrator to route traffic between the two VDOMs.(Choose two)

A. Use the inter-VDOMs links automatically created between all VDOMS.
B. Manually create and configured an inter-VDOM link between yours.
C. Interconnect and configure an external physical interface in one VDOM to another physical interface in the second VDOM.
D. Configure both VDOMs to share the same table.

Answer: BC

NEW QUESTION 174
What is the default criteria for selecting the HA master unit in a HA cluster?

A. port monitor, priority, uptime, serial number
B. Port monitor, uptime, priority, serial number
C. Priority, uptime, port monitor, serial number
D. uptime, priority, port monitor, serial number

Answer: B

NEW QUESTION 179
The exhibit shoes three static routes.

```
config router static
    edit 1
      set dst 172.20.168.0 255.255.255.0
      set distance 10
      set priority 10
     set device port1
    next
    edit 2
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port2
    next
    edit 3
      set dst 172.20.0.0 255.255.0.0
      set distance 5
      set priority 20
      set device port3
   next
end
```

Which routes will be used to route the packets to the destination IP address 172.20.168.1?

A. The route with the ID number 2 and 3.
B. Only the route with the ID number 3.
C. Only the route with the ID number 2.
D. Only the route with the ID number 1.

Answer: D

NEW QUESTION 183
In which order are firewall policies processed on a FortiGate unit?

A. From top to bottom, according with their sequence number.
B. From top to bottom, according with their policy ID number.
C. Based on best match.
D. Based on the priority value.

Answer: A

NEW QUESTION 184
If you have lost your password for the "admin" account on your FortiGate, how should you reset it?

A. Log in with another administrator account that has "super_admin" profile permissions, then reset the password for the "admin" account.
B. Reboot the FortiGat
C. Via the local console, during the boot loader, use the menu to format the flash disk and reinstall the firmwar
D. Then you can log in with the default password.
E. Power off the FortiGat
F. After several seconds, restart i
G. Via the local console, within 30 seconds after booting has completed, log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.
H. Reboot the FortiGat
I. Via the local console, during the boot loader, use the menu to log in as "maintainer" and enter the CLI commands to set the password for the "admin" account.

Answer: C

NEW QUESTION 187
Which answer best describes what an "Unknown Application" is?

A. All traffic that matches the internal signature for unknown applications.
B. Traffic that does not match the RFC pattern for its protocol.
C. Any traffic that does not match an application control signature
D. A packet that fails the CRC check.

Answer: C

NEW QUESTION 190
The exhibit shows two static routes to the same destinations subnet 172.20.168.0/24.

```
#config router static
    edit 1
      set dst 172.20.168.0 255.255.255.0
      set distance 10
       set priority 20
      set device port1
    next
    edit 2
      set dst 172.20.168.0 255.255.255.0
      set distance 20
      set priority 20
      set device port2
    next
end
```

Which of the following statements correctly describes this static routing configuration? (choose two)

A. Both routes will show up in the routing table.
B. The FortiGate unit will evenly share the traffic to 172.20.168.0/24 between routes.
C. Only one route will show up in the routing table.
D. The FortiGate will route the traffic to 172.20.168.0/24 only through one route.

Answer: CD

NEW QUESTION 195
What is valid reason for using session based authentication instead of IP based authentication in a FortiGate web proxy solution?

A. Users are required to manually enter their credentials each time they connect to a different web site.
B. Proxy users are authenticated via FSSO.
C. There are multiple users sharing the same IP address.
D. Proxy users are authenticated via RADIUS.

Answer: C

NEW QUESTION 196
A client can establish a secure connection to a corporate network using SSL VPN in tunnel mode. Which of the following statements are correct regarding the use of tunnel mode SSL VPN? (Select all that apply.)

A. Split tunneling can be enabled when using tunnel mode SSL VPN.
B. Client software is required to be able to use a tunnel mode SSL VPN.
C. Users attempting to create a tunnel mode SSL VPN connection must be authenticated by at least one SSL VPN policy.
D. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Answer: ABCD

NEW QUESTION 201
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual NSE4 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the NSE4 Product From:

https://www.2passeasy.com/dumps/NSE4/

Money Back Guarantee

NSE4 Practice Exam Features:

* NSE4 Questions and Answers Updated Frequently

* NSE4 Practice Questions Verified by Expert Senior Certified Staff

* NSE4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* NSE4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year