Vendor: Fortinet

Exam Code: FCNSP

Exam Name: Fortinet Certified Network Security Professional

Version: DEMO

QUESTION NO: 1

Which of the following is an advantage of using SNMP v3 instead of SNMP v1/v2 when querying the FortiGate unit?

A. Packet encryption

B. MIB-based report uploads

C. SNMP access limits through access lists

D. Running SNMP service on a non-standard port is possible

Answer: A

QUESTION NO: 2

An administrator logs into a FortiGate unit using an account which has been assigned a super_admin profile. Which of the following operations can this administrator perform?

A. They can delete logged-in users who are also assigned the super_admin access profile.

B. They can make changes to the super_admin profile.

C. They can delete the admin account if the default admin user is not logged in.

D. They can view all the system configuration settings but can not make changes.

E. They can access configuration options for only the VDOMs to which they have been assigned.

Answer: C

QUESTION NO: 3

The diag sys session list command is executed in the CLI. The output of this command is shown in the exhibit.

```
session info: proto=6 proto_state=11 duration=539 expire=3571 timeout=3600
flags=00000000 sockflag=00000000 sockport=80 av_idx=0 use=5
origin-shaper=guarantee-100kbps prio=1 guarantee 12288/sec max 134217728/sec
traffic 123/sec
reply-shaper=low-priority prio=3 guarantee 0/sec max 134217728/sec traffic 115/sec
per_ip_shaper=
ha_id=0 hakey=1335
policy_dir=0 tunnel=/
state=redir local may_dirty ndr os rs rem
statistic(bytes/packets/allow_err): org=3201/59/1 reply=2672/58/1 tuples=3
orgin->sink: org pre->post, reply pre->post dev=9->3/3->9
gwy=76.27.192.1/192.168.203.2
hook=post dir=org act=snat 192.168.203.2:3196-
>128.100.58.53:80(76.27.195.147:58618)
hook=pre dir=reply act=dnat 128.100.58.53:80-
>76.27.195.147:58618(192.168.203.2:3196)
hook=post dir=reply act=noop 128.100.58.53:80->192.168.203.2:3196(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=10 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=00115cae tos=ff/ff app_list=2000 app=0
dd_type=0 dd_rule_id=0
per_ip_bandwidth meter: addr=192.168.203.2, bps=1351
```

Based on the output from this command, which of the following statements is correct?

A. This is a UDP session.

B. Traffic shaping is being applied to this session.

C. This is an ICMP session.

D. This traffic has been authenticated.

E. This session matches a firewall policy with ID 5.

Answer: B

QUESTION NO: 4

A FortiGate unit is configured with multiple VDOMs. An administrative account on the device has been assigned a Scope value of VDOM:root.

Which of the following items would an administrator logging in using this account NOT be able to configure?

A. Firewall addresses

B. DHCP servers

C. FortiGuard Distribution Network configuration

D. PPTP VPN configuration

Answer: C

QUESTION NO: 5

What is the effect of using CLI "config system session-ttl" to set session_ttl to 1800 seconds?

A. Sessions can be idle for no more than 1800 seconds.

B. The maximum length of time a session can be open is 1800 seconds.

C. After 1800 seconds, the end user must reauthenticate.

D. After a session has been open for 1800 seconds, the FortiGate unit will send a keepalive packet to both client and server.

Answer: A

QUESTION NO: 6

Which of the following statements is correct about how the FortiGate unit verifies username and password during user authentication?

A. If a remote server is included in a user group, it will be checked before local accounts.

B. An administrator can define a local account for which the password must be verified by querying a remote server.

C. If authentication fails with a local password, the FortiGate unit will query the authentication server if the local user is configured with both a local password and an authentication server.

D. The FortiGate unit will only attempt to authenticate against Active Directory if Fortinet Server Authentication Extensions are installed and configured.

Answer: B

QUESTION NO: 7

Which of the following statements are correct regarding the configuration of a FortiGate unit as an SSL VPN gateway? (Select all that apply.)

A. Tunnel mode can only be used if the SSL VPN user groups have at least one Host Check option enabled.

B. The specific routes needed to access internal resources through an SSL VPN connection in tunnel mode from the client computer are defined in the routing widget associated with the SSL VPN portal.

C. In order to apply a portal to a user, that user must belong to an SSL VPN user group.

D. The portal settings specify whether the connection will operate in web-only or tunnel mode.

Answer: C,D

QUESTION NO: 8

Which of the following statements is correct about configuring web filtering overrides?

A. The Override option for FortiGuard Web Filtering is available for any user group type.

B. Admin overrides require an administrator to manually allow pending override requests which are listed in the Override Monitor.

C. The Override Scopes of User and User Group are only for use when Firewall Policy Authentication is also being used.

D. Using Web Filtering Overrides requires the use of Firewall Policy Authentication.

Answer: C

QUESTION NO: 9

The FortiGate Server Authentication Extensions (FSAE) provide 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 FSAE in a Windows domain environment when NTLM is not used? (Select all that apply.)

A. An FSAE Collector Agent must be installed on every domain controller.

B. An FSAE Domain Controller Agent must be installed on every domain controller.

C. The FSAE Domain Controller Agent will regularly update user logon information on the FortiGate unit.

D. The FSAE Collector Agent will retrieve user information from the Domain Controller Agent and will send the user logon information to the FortiGate unit.

E. For non-domain computers, an FSAE client must be installed on the computer to allow FSAE authentication.

Answer: B,D

QUESTION NO: 10

Bob wants to send Alice a file that is encrypted using public key cryptography.

Which of the following statements is correct regarding the use of public key cryptography in this scenario?

A. Bob will use his private key to encrypt the file and Alice will use her private key to decrypt the file.

B. Bob will use his public key to encrypt the file and Alice will use Bob's private key to decrypt the file.

C. Bob will use Alice's public key to encrypt the file and Alice will use her private key to decrypt the file.

D. Bob will use his public key to encrypt the file and Alice will use her private key to decrypt the

file.

E. Bob will use Alice's public key to encrypt the file and Alice will use Bob's public key to decrypt the file.

Answer: C