Exam Number/Code:FCNSP.v5

Exam Name: Fortinet Certified Network Security Professional (FCNSP.v5)

Version: Demo

QUESTION NO: 1

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 NTLM and Polling Mode are not used? (Select all that apply.)

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 retrieve user information from the Domain Controller Agent and will send the user logon information to the FortiGate unit.
E. For non-domain computers, the only way to allow FSSO authentication is to install an FSSO client.

Answer: B,D

QUESTION NO: 2

Which of the following represents the correct order of criteria used for the selection of a Master unit within a FortiGate High Availability (HA) cluster when master override is disabled?

A. 1. port monitor, 2. unit priority, 3. up time, 4. serial number
B. 1. port monitor, 2. up time, 3. unit priority, 4. serial number
C. 1. unit priority, 2. up time, 3. port monitor, 4. serial number
D. 1. up time, 2. unit priority, 3. port monitor, 4. serial number

Answer: B

QUESTION NO: 3

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 subordinate unit?

A. Request: Internal Host; Master FortiGate; Slave FortiGate; Internet; Web Server
B. Request: Internal Host; Master FortiGate; Slave FortiGate; Master FortiGate; Internet; Web Server
C. Request: Internal Host; Slave FortiGate; Internet; Web Server
D. Request: Internal Host; Slave FortiGate; Master FortiGate; Internet; Web Server

Answer: A

QUESTION NO: 4

Which of the following statements are correct regarding virtual domains (VDOMs)? (Select all that apply.)

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.
B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.
C. VDOMs share firmware versions, as well as antivirus and IPS databases.
D. Only administrative users with a 'super_admin' profile will be able to enter multiple VDOMs to make configuration changes.

Answer: A,B,C

QUESTION NO: 5

What advantages are there in using a hub-and-spoke IPSec VPN configuration instead of a fullymeshed set of IPSec tunnels? (Select all that apply.)

A. Using a hub and spoke topology is required to achieve full redundancy.
B. Using a hub and spoke topology simplifies configuration because fewer tunnels are required.
C. Using a hub and spoke topology provides stronger encryption.
D. The routing at a spoke is simpler, compared to a meshed node.

Answer: B,D

QUESTION NO: 6

Data Leak Prevention archiving gives the ability to store files and message data onto a FortiAnalyzer unit for which of the following types of network traffic? (Select all that apply.)

A. SNMP
B. IPSec
C. SMTP
D. POP3
E. HTTP

Answer: C,D,E

QUESTION NO: 7

Which of the following statements are correct regarding Application Control?

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

Answer: A,C

QUESTION NO: 8
Examine the exhibit shown below then answer the question that follows it.
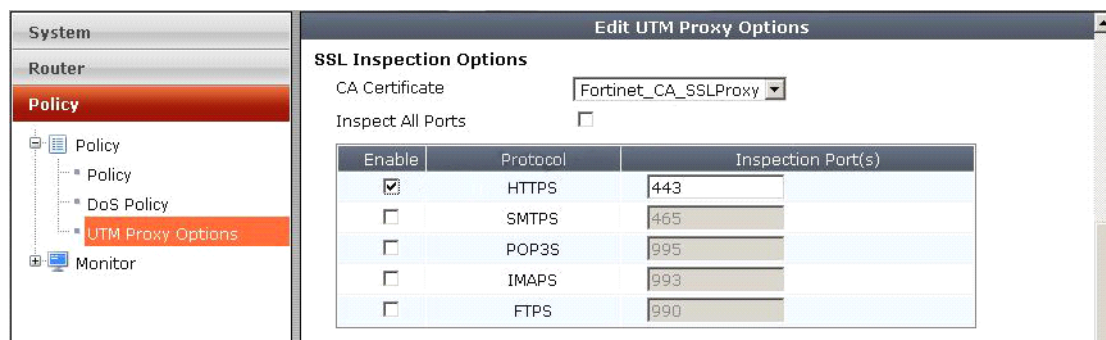
Within the UTM Proxy Options, the CA certificate Fortinet_CA_SSLProxy defines which of the following:

A. FortiGate unit's encryption certificate used by the SSL proxy.
B. FortiGate unit's signing certificate used by the SSL proxy.
C. FortiGuard's signing certificate used by the SSL proxy.
D. FortiGuard's encryption certificate used by the SSL proxy.

Answer: A

QUESTION NO: 9
For Data Leak Prevention, which of the following describes the difference between the block and quarantine actions?

A. A block action prevents the transaction. A quarantine action blocks all future transactions, regardless of the protocol.
B. A block action prevents the transaction. A quarantine action archives the data.
C. A block action has a finite duration. A quarantine action must be removed by an administrator.
D. A block action is used for known users. A quarantine action is used for unknown users.

Answer: A

QUESTION NO: 10
How can DLP file filters be configured to detect Office 2010 files? (Select all that apply.)

A. File TypE. Microsoft Office(msoffice)
B. File TypE. Archive(zip)
C. File TypE. Unknown Filetype(unknown)
D. File NamE. "*.ppt", "*.doc", "*.xls"
E. File NamE. "*.pptx", "*.docx", "*.xlsx"

Answer: B,E