Fortinet

Exam FCNSA

Fortinet Certified Network Security Administrato (V5)

Version: 7.0

[Total Questions: 119]

Question No : 1

An administrator wants to assign a set of UTM features to a group of users. Which of the following is the correct method for doing this?

A. Enable a set of unique UTM profiles under "Edit User Group".
B. The administrator must enable the UTM profiles in an identity-based policy applicable to the user group.
C. When defining the UTM objects, the administrator must list the user groups which will use the UTM object.
D. The administrator must apply the UTM features directly to a user object.

Answer: B

Question No : 2

When firewall policy authentication is enabled, only traffic on supported protocols will trigger an authentication challenge.

Select all supported protocols from the following:

A. SMTP
B. SSH
C. HTTP
D. FTP
E. SCP

Answer: C,D

Question No : 3

A client can create a secure connection to a FortiGate device using SSL VPN in web-only mode.

Which one of the following statements is correct regarding the use of web-only mode SSL VPN?

A. Web-only mode supports SSL version 3 only.
B. A Fortinet-supplied plug-in is required on the web client to use web-only mode SSL

VPN.
C. Web-only mode requires the user to have a web browser that supports 64-bit cipher length.
D. The JAVA run-time environment must be installed on the client to be able to connect to a web-only mode SSL VPN.

Answer: C

Question No : 4

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: A,B,C,D

Question No : 5

In an IPSec gateway-to-gateway configuration, two FortiGate units create a VPN tunnel between two separate private networks.

Which of the following configuration steps must be performed on both FortiGate units to support this configuration? (Select all that apply.)

A. Create firewall policies to control traffic between the IP source and destination address.
B. Configure the appropriate user groups on the FortiGate units to allow users access to the IPSec VPN connection.
C. Set the operating mode of the FortiGate unit to IPSec VPN mode.
D. Define the Phase 2 parameters that the FortiGate unit needs to create a VPN tunnel with the remote peer.

E. Define the Phase 1 parameters that the FortiGate unit needs to authenticate the remote peers.

Answer: A,D,E

Question No : 6

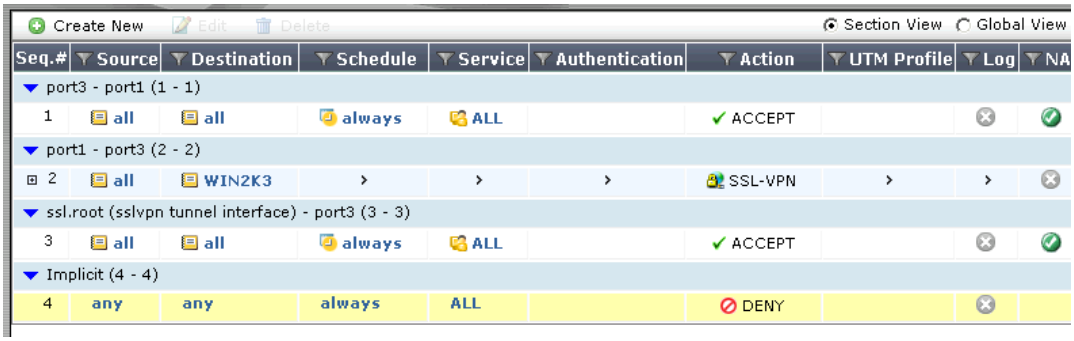
How is traffic routed onto an SSL VPN tunnel from the FortiGate unit side?

A. A static route must be configured by the administrator using the ssl.root interface as the outgoing interface.
B. Assignment of an IP address to the client causes a host route to be added to the FortiGate unit's kernel routing table.
C. A route back to the SSLVPN IP pool is automatically created on the FortiGate unit.
D. The FortiGate unit adds a route based upon the destination address in the SSL VPN firewall policy.

Answer: B

Question No : 7

An end user logs into the full-access SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has enabled split tunneling.



Given that the user authenticates against the SSL VPN policy shown in the image below, which statement below identifies the route that is added to the client's routing table.

A. A route to destination matching the 'WIN2K3' address object.
B. A route to the destination matching the 'all' address object.
C. A default route.

D. No route is added.

Answer: A

Question No : 8

Which of the following antivirus and attack definition update options are supported by FortiGate units? (Select all that apply.)

A. Manual update by downloading the signatures from the support site.
B. Pull updates from the FortiGate device
C. Push updates from the FortiGuard Distribution Network.
D. ”update-AV/AS” command from the CLI

Answer: A,B,C

Question No : 9

A FortiGate AntiVirus profile can be configured to scan for viruses on SMTP, FTP, POP3, and SMB protocols using which inspection mode?

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

Answer: C

Question No : 10

Which of the following statements regarding Banned Words are correct? (Select all that apply.)

A. The FortiGate unit can scan web pages and email messages for instances of banned words.
B. When creating a banned word list, an administrator can indicate either specific words or patterns.

C. Banned words can be expressed as simple text, wildcards or regular expressions.
D. Content is automatically blocked if a single instance of a banned word appears.
E. The FortiGate unit updates banned words on a periodic basis.

Answer: A,B,C

Question No : 11

Which statement is correct regarding virus scanning on a FortiGate unit?

A. Virus scanning is enabled by default.
B. Fortinet Customer Support enables virus scanning remotely for you.
C. Virus scanning must be enabled in a UTM security profile and the UTM security profile must be assigned to a firewall policy.
D. Enabling virus scanning in a UTM security profile enables virus scanning for all traffic flowing through the FortiGate device.

Answer: C

Question No : 12

Which of the following statements are correct regarding URL filtering on the FortiGate unit? (Select all that apply.)

A. The allowed actions for URL Filtering include Allow, Block and Exempt.
B. The allowed actions for URL Filtering are Allow and Block.
C. The FortiGate unit can filter URLs based on patterns using text and regular expressions.
D. Any URL accessible by a web browser can be blocked using URL Filtering.
E. Multiple URL Filter lists can be added to a single protection profile.

Answer: A,C

Question No : 13

Which of the following regular expression patterns will make the terms "confidential data" case insensitive?

A. \[confidential data]
B. /confidential data/i
C. i/confidential data/
D. "confidential data"
E. /confidential data/c

Answer: B

Question No : 14

Which of the following spam filtering methods are supported on the FortiGate unit? (Select all that apply.)

A. IP Address Check
B. Open Relay Database List (ORDBL)
C. Black/White List
D. Return Email DNS Check
E. Email Checksum Check

Answer: A,B,C,D,E

Question No : 15

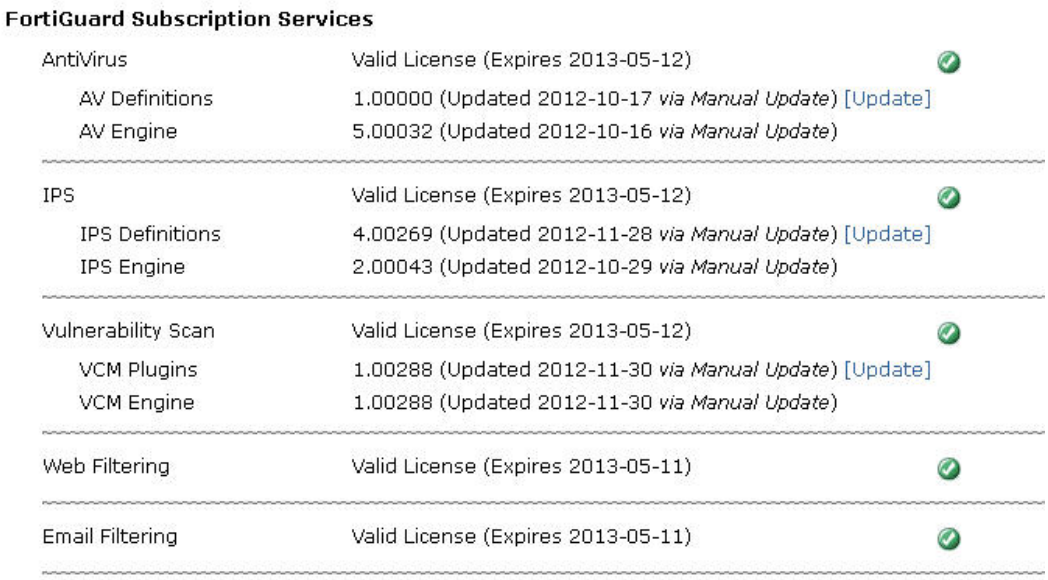
Which of the following email spam filtering features is NOT supported on a FortiGate unit?

A. Multipurpose Internet Mail Extensions (MIME) Header Check
B. HELO DNS Lookup
C. Greylisting
D. Banned Word

Answer: C

Question No : 16

Examine the exhibit shown below; then answer the question following it.



Which of the following statements best describes the green status indicators that appear next to the different FortiGuard Distribution Network services as illustrated in the exhibit?

A. They indicate that the FortiGate unit is able to connect to the FortiGuard Distribution Network.
B. They indicate that the FortiGate unit has the latest updates that are available from the FortiGuard Distribution Network.
C. They indicate that updates are available and should be downloaded from the FortiGuard Distribution Network to the FortiGate unit.
D. They indicate that the FortiGate unit is in the process of downloading updates from the FortiGuard Distribution Network.

Answer: A

Question No : 17

A FortiGate unit is configured to receive push updates from the FortiGuard Distribution Network, however, updates are not being received.

Which of the following statements are possible reasons for this? (Select all that apply.)

A. The external facing interface of the FortiGate unit is configured to use DHCP.
B. The FortiGate unit has not been registered.
C. There is a NAT device between the FortiGate unit and the FortiGuard Distribution Network and no override push IP is configured.
D. The FortiGate unit is in Transparent mode which does not support push updates.

Answer: A,B,C

Question No : 18

Which of the following statements best describes the proxy behavior on a FortiGate unit during an FTP client upload when FTP splice is disabled?

A. The proxy will not allow a file to be transmitted in multiple streams simultaneously.
B. The proxy sends the file to the server while simultaneously buffering it.
C. If the file being scanned is determined to be infected, the proxy deletes it from the server by sending a delete command on behalf of the client.
D. If the file being scanned is determined to be clean, the proxy terminates the connection and leaves the file on the server.

Answer: A

Question No : 19

A firewall policy has been configured for the internal email server to receive email from external parties through SMTP. Exhibits A and B show the antivirus and email filter profiles applied to this policy.

Exhibit A: