Fortinet

Exam NSE5

Fortinet Network Security Expert 5 Written Exam (500)

Version: 7.0

[Total Questions: 239]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	119
Topic 2: Volume B	43
Topic 3: Volume C	77

https://certkill.com

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which of the following network protocols can be used to access a FortiGate unit as an administrator?

A. HTTPS, HTTP, SSH, TELNET, PING, SNMP
B. FTP, HTTPS, NNTP, TCP, WINS
C. HTTP, NNTP, SMTP, DHCP
D. Telnet, FTP, RLOGIN, HTTP, HTTPS, DDNS
E. Telnet, UDP, NNTP, SMTP

Answer: A

Question No : 2 - (Topic 1)

Which of the following items represent the minimum configuration steps an administrator must perform to enable Data Leak Prevention for traffic flowing through the FortiGate unit? (Select all that apply.)

A. Assign a DLP sensor in a firewall policy.
B. Apply one or more DLP rules to a firewall policy.
C. Enable DLP globally using the config sys dlp command in the CLI.
D. Define one or more DLP rules.
E. Define a DLP sensor.
F. Apply a DLP sensor to a DoS sensor policy.

Answer: A,D,E

Question No : 3 - (Topic 1)

The ordering of firewall policies is very important. Policies can be re-ordered within the FortiGate Web Config and also using the CLI. The command used in the CLI to perform this function is _____.

A. set order
B. edit policy

C. reorder
D. move

Answer: D

Question No : 4 - (Topic 1)

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 : 5 - (Topic 1)

The default administrator profile that is assigned to the default "admin" user on a FortGate device is:_____.

A. trusted-admin
B. super_admin
C. super_user
D. admin
E. fortinet-root

Answer: B

Question No : 6 - (Topic 1)

Users may require access to a web site that is blocked by a policy. Administrators can give users the ability to override the block. Which of the following statements regarding overrides are correct? (Select all that apply.)

A. A protection profile may have only one user group defined as an override group.

B. A firewall user group can be used to provide override privileges for FortiGuard Web Filtering.

C. Authentication to allow the override is based on a user's membership in a user group.

D. Overrides can be allowed by the administrator for a specific period of time.

Answer: B,C,D

Question No : 7 - (Topic 1)

The command structure of the FortiGate CLI consists of commands, objects, branches, tables, and parameters. Which of the following items describes user?

A. A command.
B. An object.
C. A table.
D. A parameter.

Answer: B

Question No : 8 - (Topic 1)

Which of the following statements is correct regarding URL Filtering on the FortiGate unit?

A. The FortiGate unit can filter URLs based on patterns using text and regular expressions.
B. The available actions for URL Filtering are Allow and Block.
C. Multiple URL Filter lists can be added to a single Web filter profile.
D. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.

Answer: A

Question No : 9 - (Topic 1)

UTM features can be applied to which of the following items?

A. Firewall policies
B. User groups

C. Policy routes

D. Address groups

Answer: A

A FortiGate unit can create a secure connection to a client 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. Software must be downloaded to the web client to be able to use a tunnel mode SSL VPN.

C. Users attempting to create a tunnel mode SSL VPN connection must be members of a configured user group on the FortiGate unit.

D. Tunnel mode SSL VPN requires the FortiClient software to be installed on the user's computer.

E. The source IP address used by the client for the tunnel mode SSL VPN is assigned by the FortiGate unit.

Answer: A,B,C,E

The FortiGate unit's GUI provides a link to update the firmware.

Clicking this link will perform which of the following actions?

A. It will connect to the Fortinet Support site where the appropriate firmware version can be selected.

B. It will send a request to the FortiGuard Distribution Network so that the appropriate firmware version can be pushed down to the FortiGate unit.

C. It will present a prompt to allow browsing to the location of the firmware file.

D. It will automatically connect to the Fortinet Support site to download the most recent firmware version for the FortiGate unit.

Answer: C

Question No : 12 - (Topic 1)

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 : 13 - (Topic 1)

The ordering of firewall policies is very important. Policies can be re-ordered within the FortiGate unit's GUI and also using the CLI. The command used in the CLI to perform this function is _____ .

A. set order
B. edit policy
C. reorder
D. move

Answer: D

Question No : 14 - (Topic 1)

Which of the following statements are correct regarding logging to memory on a FortiGate unit? (Select all that apply.)

A. When the system has reached its capacity for log messages, the FortiGate unit will stop logging to memory.

B. When the system has reached its capacity for log messages, the FortiGate unit overwrites the oldest messages.
C. If the FortiGate unit is reset or loses power, log entries captured to memory will be lost.
D. None of the above.

Answer: B,C

Question No : 15 - (Topic 1)

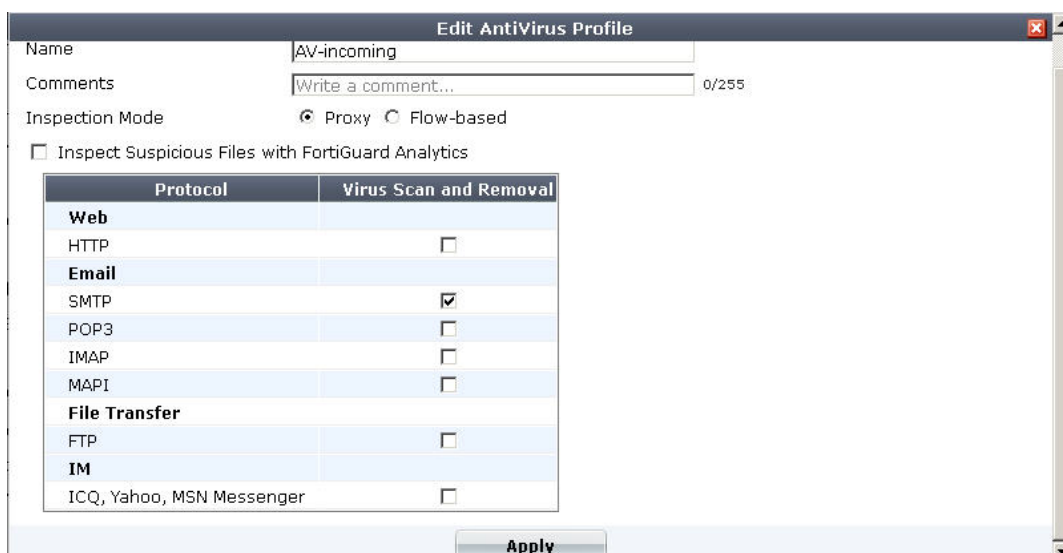A FortiAnalyzer device could use which security method to secure the transfer of log data from FortiGate devices?

A. SSL
B. IPSec
C. direct serial connection
D. S/MIME

Answer: B

Question No : 16 - (Topic 1)

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:

Exhibit B:

What is the correct behavior when the email attachment is detected as a virus by the FortiGate antivirus engine?

A. The FortiGate unit will remove the infected file and deliver the email with a replacement message to alert the recipient that the original attachment was infected.
B. The FortiGate unit will reject the infected email and the sender will receive a failed delivery message.
C. The FortiGate unit will remove the infected file and add a replacement message. Both sender and recipient are notified that the infected file has been removed.
D. The FortiGate unit will reject the infected email and notify the sender.

Answer: B

Question No : 17 - (Topic 1)

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 : 18 - (Topic 1)

Two-factor authentication is supported using the following methods? (Select all that apply.)

A. FortiToken
B. Email
C. SMS phone message
D. Code books

Answer: A,B,C

Question No : 19 - (Topic 1)

SSL content inspection is enabled on the FortiGate unit. Which of the following steps is required to prevent a user from being presented with a web browser warning when accessing an SSL-encrypted website?

A. The root certificate of the FortiGate SSL proxy must be imported into the local certificate store on the user's workstation.
B. Disable the strict server certificate check in the web browser under Internet Options.
C. Enable transparent proxy mode on the FortiGate unit.
D. Enable NTLM authentication on the FortiGate unit. NTLM authentication suppresses the certificate warning messages in the web browser.

Answer: A

Question No : 20 - (Topic 1)

Which of the following options can you use to update the virus definitions on a FortiGate unit? (Select all that apply.)

A. Push update
B. Scheduled update
C. Manual update
D. FTP update