

Certkiller FCNSA.v5 119q

Number: FCNSA.v5
Passing Score: 800
Time Limit: 120 min
File Version: 16.5

Fortinet FCNSA.v5

Fortinet Certified Network Security Administrator (V5)



100% Valid in US, UK, Australia, India and Emirates. All my friends in group have these same questions.

Exam A

QUESTION 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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.
Real 2
Fortinet FCNSA.v5 Exam
- D. The JAVA run-time environment must be installed on the client to be able to connect to a web- only mode SSL VPN.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Correct Answer: ABCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Real 3

Fortinet FCNSA.v5 Exam

Explanation:

QUESTION 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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Seq.#	Source	Destination	Schedule	Service	Authentication	Action	UTM Profile	Log	NA
port3 - port1 (1 - 1)									
1	all	all	always	ALL		ACCEPT			
port1 - port3 (2 - 2)									
2	all	WIN2K3				SSL-VPN			
ssl.root (sslvpn tunnel interface) - port3 (3 - 3)									
3	all	all	always	ALL		ACCEPT			
Implicit (4 - 4)									
4	any	any	always	ALL		DENY			

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.

Real 4
Fortinet FCNSA.v5 Exam

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 13

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

Real 6

Fortinet FCNSA.v5 Exam

- A. \[confidential data]
- B. /confidential data/i
- C. i/confidential data/

- D. "confidential data"
- E. /confidential data/c

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: A,B,C,D,E
Explanation:

QUESTION 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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 16

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

Real 7

Fortinet FCNSA.v5 Exam

FortiGuard Subscription Services

AntiVirus	Valid License (Expires 2013-05-12)	
AV Definitions	1.00000 (Updated 2012-10-17 via Manual Update) [Update]	
AV Engine	5.00032 (Updated 2012-10-16 via Manual Update)	
<hr/>		
IPS	Valid License (Expires 2013-05-12)	
IPS Definitions	4.00269 (Updated 2012-11-28 via Manual Update) [Update]	
IPS Engine	2.00043 (Updated 2012-10-29 via Manual Update)	
<hr/>		
Vulnerability Scan	Valid License (Expires 2013-05-12)	
VCM Plugins	1.00288 (Updated 2012-11-30 via Manual Update) [Update]	
VCM Engine	1.00288 (Updated 2012-11-30 via Manual Update)	
<hr/>		
Web Filtering	Valid License (Expires 2013-05-11)	
<hr/>		
Email Filtering	Valid License (Expires 2013-05-11)	
<hr/>		

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Real 8

Fortinet FCNSA.v5 Exam

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 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.

Correct Answer: A

Section: (none)

Explanation

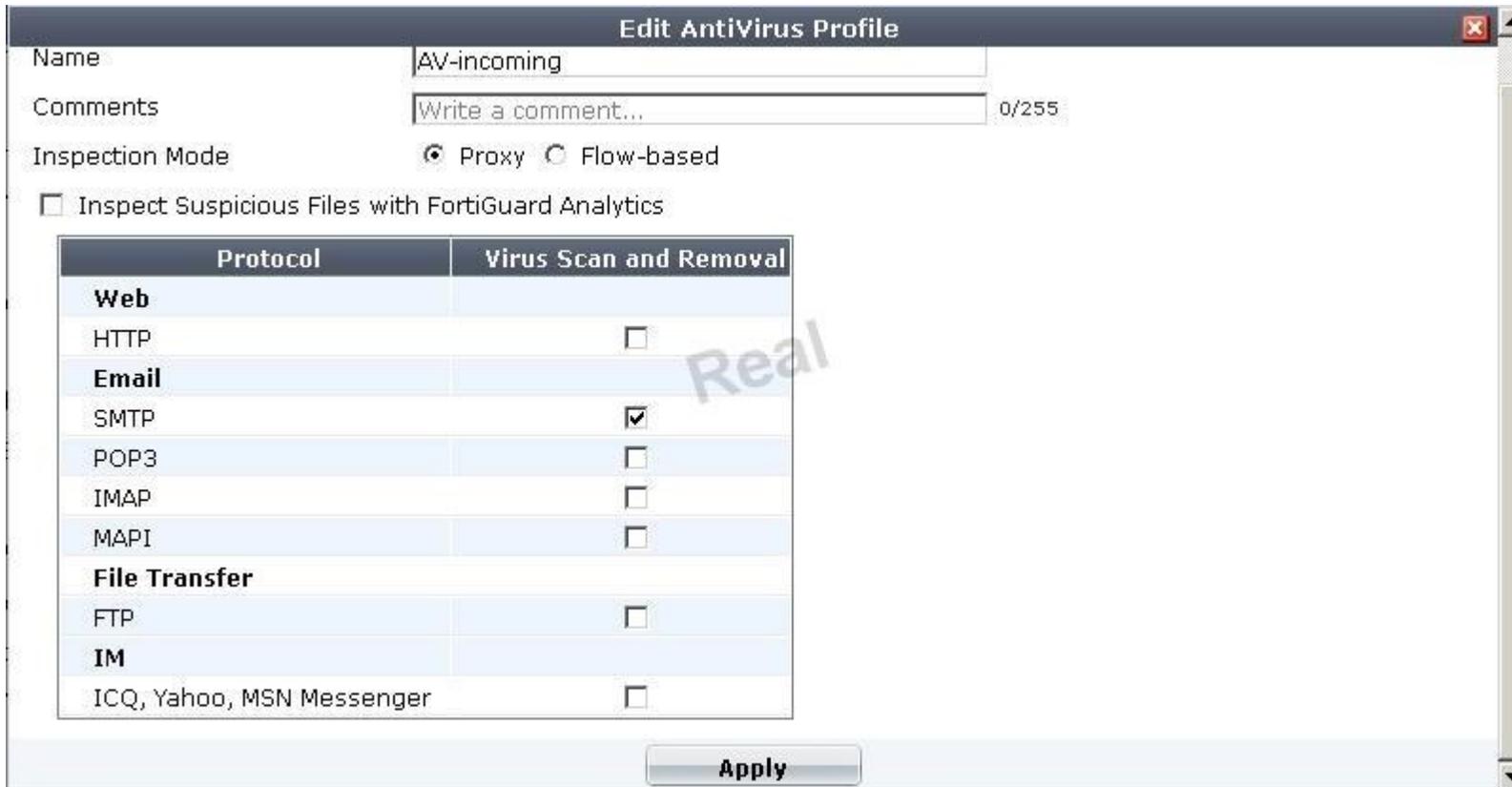
Explanation/Reference:

Explanation:

QUESTION 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:



Edit AntiVirus Profile

Name: AV-incoming

Comments: Write a comment... 0/255

Inspection Mode: Proxy Flow-based

Inspect Suspicious Files with FortiGuard Analytics

Protocol	Virus Scan and Removal
Web	
HTTP	<input type="checkbox"/>
Email	
SMTP	<input checked="" type="checkbox"/>
POP3	<input type="checkbox"/>
IMAP	<input type="checkbox"/>
MAPI	<input type="checkbox"/>
File Transfer	
FTP	<input type="checkbox"/>
IM	
ICQ, Yahoo, MSN Messenger	<input type="checkbox"/>

Apply

Real 9
 Fortinet FCNSA.v5 Exam
 Exhibit B:

View Email Filter Profile ✕

Name

Comments 0/255

Inspection Mode Proxy Flow-based

Enable Spam Detection and Filtering

	<input checked="" type="checkbox"/> IMAP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> SMTP
Spam Action	Tagged	Tagged	Discard ▼
Tag Location	Subject ▼	Subject ▼	Subject ▼
Tag Format	Spam	Spam	Spam

▶ FortiGuard Spam Filtering

▶ Local Spam Filtering

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 20

Which email filter is NOT available on a FortiGate device?

- A. Sender IP reputation database.
- B. URLs included in the body of known SPAM messages.
- C. Email addresses included in the body of known SPAM messages.
- D. Spam object checksums.
- E. Spam grey listing.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 10

Fortinet FCNSA.v5 Exam

QUESTION 21

Which part of an email message exchange is NOT inspected by the POP3 and IMAP proxies?

- A. TCP connection
- B. File attachments
- C. Message headers
- D. Message body

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 22

What are the valid sub-types for a Firewall type policy? (Select all that apply)

- A. Device Identity

- B. Address
- C. User Identity
- D. Schedule
- E. SSL VPN

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 23

In NAT/Route mode when there is no matching firewall policy for traffic to be forwarded by the Firewall, which of the following statements describes the action taken on traffic?

- A. The traffic is blocked.
- B. The traffic is passed.
- C. The traffic is passed and logged.
- D. The traffic is blocked and logged.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 11

Fortinet FCNSA.v5 Exam

QUESTION 24

In which order are firewall policies processed on the FortiGate unit?

- A. They are processed from the top down according to their sequence number.
- B. They are processed based on the policy ID number shown in the left hand column of the policy window.
- C. They are processed on best match.
- D. They are processed based on a priority value assigned through the priority column in the policy window.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25

Which of the following pieces of information can be included in the Destination Address field of a firewall policy? (Select all that apply.)

- A. An IP address pool.
- B. A virtual IP address.
- C. An actual IP address or an IP address group.
- D. An FQDN or Geographic value(s).

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26

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
- Real 12
Fortinet FCNSA.v5 Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 27

You wish to create a firewall policy that applies only to traffic intended for your web server. The web server has an IP address of 192.168.2.2 and a /24

subnet mask. When defining the firewall address for use in this policy, which one of the following addresses is correct?

- A. 192.168.2.0 / 255.255.255.0
- B. 192.168.2.2 / 255.255.255.0
- C. 192.168.2.0 / 255.255.255.255
- D. 192.168.2.2 / 255.255.255.255

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 28

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 29

Which of the following network protocols are supported for administrative access to a FortiGate unit?

- 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30

Which of the following statements is correct regarding a FortiGate unit operating in NAT/Route mode?

- A. The FortiGate unit applies NAT to all traffic.
- B. The FortiGate unit functions as a Layer 3 device.
- C. The FortiGate unit functions as a Layer 2 device.
- D. The FortiGate unit functions as a router and the firewall function is disabled.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31

A FortiGate unit can provide which of the following capabilities? (Select all that apply.)

- A. Email filtering
- B. Firewall
- C. VPN gateway
- D. Mail relay
- E. Mail server

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32

Which of the following methods can be used to access the CLI? (Select all that apply.)

- A. By using a direct connection to a serial console.
- B. By using the CLI console window in the GUI.
Real 14
Fortinet FCNSA.v5 Exam
- C. By using an SSH connection.
- D. By using a Telnet connection.

Correct Answer: ABCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 33

CORRECT TEXT

The _____ CLI command is used on the FortiGate unit to run static commands such as ping or to reset the FortiGate unit to factory defaults.

- A.
- B.
- C.
- D.

Correct Answer:

Section: (none)

Explanation

Explanation/Reference:

Answer: execute

QUESTION 34

When backing up the configuration file on a FortiGate unit, the contents can be encrypted by enabling the encrypt option and supplying a password.

If the password is forgotten, the configuration file can still be restored using which of the following methods?

- A. Selecting the recover password option during the restore process.
- B. Having the password emailed to the administrative user by selecting the Forgot Password option.
- C. Sending the configuration file to Fortinet Support for decryption.
- D. If the password is forgotten, there is no way to use the file.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 35

When creating administrative users which of the following configuration objects determines access rights on the FortiGate unit.

- A. profile
 - B. allowaccess interface settings
 - C. operation mode
 - D. local-in policy
- Real 15
Fortinet FCNSA.v5 Exam

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 36

What is the FortiGate unit password recovery process?

- A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.
- B. Log in through the console port using the "maintainer" account within approximately 30 seconds of a reboot.
- C. Hold down the CTRL + Esc (Escape) keys during reboot, then reset the admin password.
- D. The only way to regain access is to interrupt the boot sequence and restore a configuration file for which the password has been modified.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 37

Which of the following statements are true of the FortiGate unit's factory default configuration?

- A. `Port1' or `Internal' interface will have an IP of 192.168.1.99.
- B. `Port1' or `Internal' interface will have a DHCP server set up and enabled (on devices that support DHCP Servers).
- C. Default login will always be the username: admin (all lowercase) and no password.
- D. The implicit firewall action is ACCEPT.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 38

Under the System Information widget on the dashboard, which of the following actions are available for the system configuration? (Select all that apply.)

- A. Backup
- B. Restore
Real 16
Fortinet FCNSA.v5 Exam
- C. Revisions
- D. Export

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 39

Encrypted backup files provide which of the following benefits? (Select all that apply.)

- A. Integrity of the backup file is protected since it cannot be easily modified when encrypted.
- B. Prevents the backup file from becoming corrupted.
- C. Protects details of the device's configuration settings from being discovered while the backup file is in transit. For example, transferred to a data centers for system recovery.
- D. A copy of the encrypted backup file is automatically pushed to the FortiGuard Distribution Service (FDS) for disaster recovery purposes. If the backup file becomes corrupt it can be retrieved through FDS.

E. Fortinet Technical Support can recover forgotten passwords with a backdoor passphrase.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 40

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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 17

Fortinet FCNSA.v5 Exam

QUESTION 41

Which of the following products is designed to manage multiple FortiGate devices?

- A. FortiGate device
- B. FortiAnalyzer device
- C. FortiClient device
- D. FortiManager device
- E. FortiMail device
- F. FortiBridge device

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 42

Which of the following products provides dedicated hardware to analyze log data from multiple FortiGate devices?

- A. FortiGate device
- B. FortiAnalyzer device
- C. FortiClient device
- D. FortiManager device
- E. FortiMail device
- F. FortiBridge device

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 43

Which of the following are valid FortiGate device interface methods for handling DNS requests? (Select all that apply.)

- A. Forward-only
 - B. Non-recursive
 - C. Recursive
 - D. Iterative
 - E. Conditional-forward
- Real 18
Fortinet FCNSA.v5 Exam

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 44

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 45

Which of the following logging options are supported on a FortiGate unit? (Select all that apply.)

- A. LDAP
- B. Syslog
- C. FortiAnalyzer
- D. Local disk and/or memory

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 46

In order to match an identity-based policy, the FortiGate unit checks the IP information. Once inside the policy, the following logic is followed:

- A. First, a check is performed to determine if the user's login credentials are valid. Next, the user is checked to determine if they belong to any of the groups defined for that policy. Finally, user restrictions are determined and port, time, and UTM profiles are applied.
 - B. First, user restrictions are determined and port, time, and UTM profiles are applied. Next, a Real 19
- Fortinet FCNSA.v5 Exam

check is performed to determine if the user's login credentials are valid. Finally, the user is checked to determine if they belong to any of the groups defined for that policy.

- C. First, the user is checked to determine if they belong to any of the groups defined for that policy. Next, user restrictions are determined and port, time, and UTM profiles are applied. Finally, a check is performed to determine if the user's login credentials are valid.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 47

Which of the following statements regarding the firewall policy authentication timeout is true?

- A. The authentication timeout is an idle timeout. This means that the FortiGate unit will consider a user to be "idle" if it does not see any packets coming from the user's source IP.
- B. The authentication timeout is a hard timeout. This means that the FortiGate unit will remove the temporary policy for this user's source IP after this timer has expired.
- C. The authentication timeout is an idle timeout. This means that the FortiGate unit will consider a user to be "idle" if it does not see any packets coming from the user's source MAC.
- D. The authentication timeout is a hard timeout. This means that the FortiGate unit will remove the temporary policy for this user's source MAC after this timer has expired.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 48

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

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 49

Real 20

Fortinet FCNSA.v5 Exam

Which of the following statements are true regarding Local User Authentication? (Select all that apply.)

- A. Local user authentication is based on usernames and passwords stored locally on the FortiGate unit.
- B. Two-factor authentication can be enabled on a per user basis.
- C. Administrators can create an account for the user locally and specify the remote server to verify the password.
- D. Local users are for administration accounts only and cannot be used for identity policies.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 50

Which of the statements below are true regarding firewall policy disclaimers? (Select all that apply.)

- A. User must accept the disclaimer to proceed with the authentication process.
- B. The disclaimer page is customizable.
- C. The disclaimer cannot be used in combination with user authentication.
- D. The disclaimer can only be applied to wireless interfaces.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 51

Examine the firewall configuration shown below; then answer the question following it.

Seq.#	From	To	Source	Destination	Service	Action	Schedule	Authentication	NAT	Log	UTM Prof
1	port3	port1	all			ACCEPT					
1.1				all	ALL		always	training			
2	any	any	any	any	ALL	DENY	always				

Which of the following statements are correct based on the firewall configuration illustrated in the exhibit? (Select all that apply.)

- A. A user can access the Internet using only the protocols that are supported by user authentication.
- B. A user can access the Internet using any protocol except HTTP, HTTPS, Telnet, and FTP. These require authentication before the user will be allowed access.
- C. A user must authenticate using the HTTP, HTTPS, SSH, FTP, or Telnet protocol before they can access any services.
- D. A user cannot access the Internet using any protocols unless the user has passed firewall authentication.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 52

When browsing to an internal web server using a web-mode SSL VPN bookmark, from which of the following source IP addresses would the web server consider the HTTP request to be initiated?

- A. The remote user's virtual IP address.
- B. The FortiGate unit's internal IP address.
- C. The remote user's public IP address.
- D. The FortiGate unit's external IP address.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 53

An issue could potentially occur when clicking Connect to start tunnel mode SSL VPN. The tunnel will start up for a few seconds, then shut down.

Which of the following statements best describes how to resolve this issue?

- A. This user does not have permission to enable tunnel mode. Make sure that the tunnel mode widget has been added to that user's web portal.
- B. This FortiGate unit may have multiple Internet connections. To avoid this problem, use the appropriate CLI command to bind the SSL VPN connection to the original incoming interface.
- C. Check the SSL adaptor on the host machine. If necessary, uninstall and reinstall the adaptor from the tunnel mode portal.
- D. Make sure that only Internet Explorer is used. All other browsers are unsupported.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 22

Fortinet FCNSA.v5 Exam

QUESTION 54

You are the administrator in charge of a FortiGate unit which acts as a VPN gateway. You have chosen to use Interface Mode when configuring the VPN tunnel and you want users from either side to be able to initiate new sessions. There is only 1 subnet at either end and the FortiGate unit already has a default route.

Which of the following configuration steps are required to achieve these objectives? (Select all that apply.)

- A. Create one firewall policy.
- B. Create two firewall policies.
- C. Add a route for the remote subnet.
- D. Add a route for incoming traffic.
- E. Create a phase 1 definition.
- F. Create a phase 2 definition.

Correct Answer: BCEF

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 55

Which of the following items is NOT a packet characteristic matched by a firewall service object?

- A. ICMP type and code
- B. TCP/UDP source and destination ports
- C. IP protocol number
- D. TCP sequence number

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 56

A firewall policy has been configured such that traffic logging is disabled and a UTM function is enabled.

Real 23

Fortinet FCNSA.v5 Exam

In addition, the system setting `utm-incident-traffic-log' has been enabled. In which log will a UTM event message be stored?

- A. Traffic
- B. UTM
- C. System
- D. None

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 57

Which one of the following statements is correct about raw log messages?

- A. Logs have a header and a body section. The header will have the same layout for every log message. The body section will change layout from one type of log message to another.
- B. Logs have a header and a body section. The header and body will change layout from one type of log message to another.

C. Logs have a header and a body section. The header and body will have the same layout for every log message.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 58

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 24

Fortinet FCNSA.v5 Exam

QUESTION 59

Which of the following authentication types are supported by FortiGate units? (Select all that apply.)

- A. Kerberos
- B. LDAP
- C. RADIUS
- D. Local Users

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 60

Which of the following are valid authentication user group types on a FortiGate unit? (Select all that apply.)

- A. Firewall
- B. Directory Service
- C. Local
- D. LDAP
- E. PKI

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 61

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.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 25

Fortinet FCNSA.v5 Exam

QUESTION 62

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 is NOT correct?

- A. A web filter profile may only have 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. When requesting an override, the matched user must belong to a user group for which the override capability has been enabled.
- D. Overrides can be allowed by the administrator for a specific period of time.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 63

An administrator has configured a FortiGate unit so that end users must authenticate against the firewall using digital certificates before browsing the Internet. What must the user have for a successful authentication? (Select all that apply.)

- A. An entry in a supported LDAP Directory.
- B. A digital certificate issued by any CA server.
- C. A valid username and password.
- D. A digital certificate issued by the FortiGate unit.
- E. Membership in a firewall user group.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 64

The FortiGate unit can be configured to allow authentication to a RADIUS server. The RADIUS server can use several different authentication protocols during the authentication process.

Which of the following are valid authentication protocols that can be used when a user authenticates to the RADIUS server? (Select all that apply.)

Real 26

Fortinet FCNSA.v5 Exam

- A. MS-CHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol v2)
- B. PAP (Password Authentication Protocol)
- C. CHAP (Challenge-Handshake Authentication Protocol)

- D. MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol v1)
- E. FAP (FortiGate Authentication Protocol)

Correct Answer: ABCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 65

Which of the following are valid components of the Fortinet Server Authentication Extensions (FSAE)? (Select all that apply.)

- A. Domain Local Security Agent.
- B. Collector Agent.
- C. Active Directory Agent.
- D. User Authentication Agent.
- E. Domain Controller Agent.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 66

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.

Correct Answer: ABCE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 27

Fortinet FCNSA.v5 Exam

QUESTION 67

An end user logs into the SSL VPN portal and selects the Tunnel Mode option by clicking on the "Connect" button. The administrator has not enabled split tunneling and so the end user must access the Internet through the SSL VPN Tunnel.

Which firewall policies are needed to allow the end user to not only access the internal network but also reach the Internet?

A.

	Status	ID	Source	Destination	Schedule	Service	Action
▼ ssl.root -> internal (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY	ACCEPT
▼ ssl.root -> wan1 (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	3	all	all	always	ANY	ACCEPT
▼ wan1 -> internal (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY	SSL-VPN
▶ Implicit (1)							

B.

[Column Settings]							
	Status	ID	Source	Destination	Schedule	Service	Action
▼ ssl.root -> internal (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY	SSL-VPN
▼ ssl.root -> wan1 (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	3	all	all	always	ANY	SSL-VPN
▼ wan1 -> internal (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY	SSL-VPN
▶ Implicit (1)							

C.

[Column Settings]							
	Status	ID	Source	Destination	Schedule	Service	Action
▼ wan1 -> internal (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY	SSL-VPN
▼ wan1 -> wan1 (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY	SSL-VPN
▶ Implicit (1)							

D. Real 28
Fortinet FCNSA.v5 Exam

[Column Settings]							
	Status	ID	Source	Destination	Schedule	Service	Action
▼ wan1 -> internal (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	all	all	always	ANY	ACCEPT
▼ wan1 -> wan1 (1)							
<input type="checkbox"/>	<input checked="" type="checkbox"/>	2	all	all	always	ANY	ACCEPT
▶ Implicit (1)							

- A. Exhibit A
- B. Exhibit B
- C. Exhibit C
- D. Exhibit D

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 68

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

- A. Manual, user-initiated updates from the FortiGuard Distribution Network.
- B. Hourly, daily, or weekly scheduled antivirus and attack definition and antivirus engine updates from the FortiGuard Distribution Network.
- C. Push updates from the FortiGuard Distribution Network.
- D. Update status including version numbers, expiry dates, and most recent update dates and times.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 69

By default the Intrusion Protection System (IPS) on a FortiGate unit is set to perform which action?

- A. Block all network attacks.
- B. Block the most common network attacks.
- C. Allow all traffic.
- D. Allow and log all traffic.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Real 29
Fortinet FCNSA.v5 Exam

Explanation:

QUESTION 70

A FortiGate unit can scan for viruses on which types of network traffic? (Select all that apply.)

- A. POP3
- B. FTP
- C. SMTP
- D. SNMP
- E. NetBios

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 71

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 wildcards or regular expressions.
- D. Content is automatically blocked if a single instance of a banned word appears.
- E. The FortiGate unit includes a pre-defined library of common banned words.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 72

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 protection profile and the protection profile must be assigned to a firewall policy.
- D. Enabling virus scanning in a protection profile enables virus scanning for all traffic flowing Real 30 Fortinet FCNSA.v5 Exam through the FortiGate.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 73

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

- A. The available actions for URL Filtering are Allow and Block.
- B. Multiple URL Filter lists can be added to a single Web filter profile.
- C. A FortiGuard Web Filtering Override match will override a block action in the URL filter list.
- D. The available actions for URL Filtering are Allow, Block and Exempt.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 74

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 75

Which of the following Regular Expression patterns will make the term "bad language" case insensitive?

- A. [bad language]
- B. /bad language/i
- C. i/bad language/
- D. "bad language"
Real 31
Fortinet FCNSA.v5 Exam
- E. /bad language/c

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 76

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.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 77

Which of the following statements describes the method of creating a policy to block access to an FTP site?

- A. Enable Web Filter URL blocking and add the URL of the FTP site to the URL Block list.
- B. Create a firewall policy with destination address set to the IP address of the FTP site, the Service set to FTP, and the Action set to Deny.
- C. Create a firewall policy with a protection profile containing the Block FTP option enabled.
- D. None of the above.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 78

Real 32

Fortinet FCNSA.v5 Exam

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

- A. Firewall policies
- B. User groups
- C. Policy routes
- D. Address groups

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 79

Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function. How are UTM features applied to traffic?

- A. One or more UTM features are enabled in a firewall policy.
- B. In the system configuration for that UTM feature, you can identify the policies to which the feature is to be applied.
- C. Enable the appropriate UTM objects and identify one of them as the default.
- D. For each UTM object, identify which policy will use it.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 80

If no firewall policy is specified between two FortiGate interfaces and zones are not used, which of the following statements describes the action taken on traffic flowing between these interfaces?

- A. The traffic is blocked.
- B. The traffic is passed.
- C. The traffic is passed and logged.
- D. The traffic is blocked and logged.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 81

Real 33

Fortinet FCNSA.v5 Exam

In which order are firewall policies processed on the FortiGate unit?

- A. They are processed from the top down as they appear in Web Config.
- B. They are processed based on the policy ID number shown in the left hand column of the policy window.
- C. They are processed using a policy hierarchy scheme that allows for multiple decision branching.
- D. They are processed based on a priority value assigned through the priority column in the policy window.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 82

File blocking rules are applied before which of the following?

- A. Firewall policy processing
- B. Virus scanning
- C. Web URL filtering
- D. White/Black list filtering

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 83

Which of the following pieces of information can be included in the Destination Address field of a firewall policy?

- A. An IP address pool, a virtual IP address, an actual IP address, and an IP address group.
- B. A virtual IP address, an actual IP address, and an IP address group.
- C. An actual IP address and an IP address group.
- D. Only an actual IP address.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 34

Fortinet FCNSA.v5 Exam

QUESTION 84

FortiGate units are preconfigured with four default protection profiles. These protection profiles are used to control the type of content inspection to be performed.

What action must be taken for one of these profiles to become active?

- A. The protection profile must be assigned to a firewall policy.
- B. The "Use Protection Profile" option must be selected in the Web Config tool under the sections for AntiVirus, IPS, WebFilter, and AntiSpam.
- C. The protection profile must be set as the Active Protection Profile.
- D. All of the above.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 85

A FortiGate 60 unit is configured for your small office. The DMZ interface is connected to a network containing a web server and email server. The Internal interface is connected to a network containing 10 user workstations and the WAN1 interface is connected to your ISP.

You want to configure firewall policies so that your users can send and receive email messages to the email server on the DMZ network. You also want the email server to be able to retrieve email messages from an email server hosted by your ISP using the POP3 protocol.

Which policies must be created for this communication? (Select all that apply.)

- A. Internal > DMZ
- B. DMZ > Internal
- C. Internal > WAN1
- D. WAN1 > Internal
- E. DMZ > WAN1
- F. WAN1 > DMZ

Correct Answer: AE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 86

Real 35

Fortinet FCNSA.v5 Exam

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 87

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 88

Which of the following statements is correct regarding a FortiGate unit operating in NAT/Route mode?

- A. The FortiGate unit requires only a single IP address for receiving updates and configuring from a management computer.
- B. The FortiGate unit must use public IP addresses on both the internal and external networks.
- C. The FortiGate unit commonly uses private IP addresses on the internal network but hides them using network address translation.
- D. The FortiGate unit uses only DHCP-assigned IP addresses on the internal network.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 36

Fortinet FCNSA.v5 Exam

QUESTION 89

Which of the following statements correctly describes how a FortiGate unit functions in Transparent mode?

- A. To manage the FortiGate unit, one of the interfaces must be designated as the management interface. This interface may not be used for forwarding data.
- B. An IP address is used to manage the FortiGate unit but this IP address is not associated with a specific interface.
- C. The FortiGate unit must use public IP addresses on the internal and external networks.
- D. The FortiGate unit uses private IP addresses on the internal network but hides them using address translation.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 90

The Idle Timeout setting on a FortiGate unit applies to which of the following?

- A. Web browsing
- B. FTP connections
- C. User authentication
- D. Administrator access
- E. Web filtering overrides.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 91

You wish to create a firewall policy that applies only to traffic intended for your web server. The server has an IP address of 192.168.2.2 and belongs to a class C subnet. When defining the firewall address for use in this policy, which one of the following addressing formats is correct?

- A. 192.168.2.0 / 255.255.255.0
 - B. 192.168.2.2 / 255.255.255.0
- Real 37

Fortinet FCNSA.v5 Exam

- C. 192.168.2.0 / 255.255.255.255
- D. 192.168.2.2 / 255.255.255.255

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 92

If a FortiGate unit has a dmz interface IP address of 210.192.168.2 with a subnet mask of 255.255.255.0, what is a valid dmz DHCP addressing range?

- A. 172.168.0.1 - 172.168.0.10
- B. 210.192.168.3 - 210.192.168.10
- C. 210.192.168.1 - 210.192.168.4
- D. All of the above.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 93

A FortiGate unit can act as which of the following? (Select all that apply.)

- A. Antispam filter
- B. Firewall
- C. VPN gateway
- D. Mail relay
- E. Mail server

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 94

Which of the following components are contained in all FortiGate units from the FG50 models and up? (Select all that apply.)

- A. FortiASIC content processor.
Real 38
Fortinet FCNSA.v5 Exam
- B. Hard Drive.
- C. Gigabit network interfaces.
- D. Serial console port.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 95

Which of the following methods can be used to access the CLI? (Select all that apply.)

- A. By using a direct connection to a serial console.
- B. By using the CLI console window in Web Config.
- C. By using an SSH connection.
- D. By using a Telnet connection.

Correct Answer: ABCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 96

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97

The command structure of the CLI on a FortiGate unit consists of commands, objects, branches, tables and parameters. Which of the following items describes port1?

- A. A command.
Real 39
Fortinet FCNSA.v5 Exam
- B. An object.
- C. A table.
- D. A parameter.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98

CORRECT TEXT

When creating administrative users, the assigned _____ determines user rights on the FortiGate unit.

- A.
- B.
- C.
- D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

Answer: access profile

QUESTION 99

Each UTM feature has configurable UTM objects such as sensors, profiles or lists that define how the feature will function.

An administrator must 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 features under "Edit User Group".
- B. The administrator must enable the UTM features in an identify-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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 100

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.)

Real 40

Fortinet FCNSA.v5 Exam

- 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.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 101

Because changing the operational mode to Transparent resets device (or vdom) to all defaults, which precautions should an Administrator take prior to performing this? (Select all that apply.)

- A. Backup the configuration.
- B. Disconnect redundant cables to ensure the topology will not contain layer 2 loops.
- C. Set the unit to factory defaults.
- D. Update IPS and AV files.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 102

Which of the following is true regarding Switch Port Mode?

- A. Allows all internal ports to share the same subnet.
- B. Provides separate routable interfaces for each internal port.
- C. An administrator can select ports to be used as a switch.
- D. Configures ports to be part of the same broadcast domain.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 103

What is the FortiGate unit password recovery process?

Real 41

Fortinet FCNSA.v5 Exam

- A. Interrupt boot sequence, modify the boot registry and reboot. After changing the password, reset the boot registry.

- B. Log in through the console port using the maintainer account within several minutes of a reboot.
- C. Hold CTRL + break during reboot and reset the admin password.
- D. The only way to regain access is to interrupt boot sequence and restore a configuration file for which the password has been modified.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 104

The FortiGate Web Config provides a link to update the firmware in the System > Status window. 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.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 105

Which of the following statements correctly describes how a push update from the FortiGuard Distribution Network (FDN) works?

- A. The FDN sends push updates only once.
- B. The FDN sends package updates automatically to the FortiGate unit without requiring an update request.
- C. The FDN continues to send push updates until the FortiGate unit sends an acknowledgement.
- D. The FDN sends a message to the FortiGate unit that there is an update available and that the FortiGate unit should download the update.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 42
Fortinet FCNSA.v5 Exam

QUESTION 106

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

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 107

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

Backup & Restore Revision Control **FortiGuard**

FortiGuard Distribution Network

Support Contract		
Availability	Valid Contract FortiOS 3.000 (Expires 2009-03-11)	
FortiGuard Subscription Services		
AntiVirus	Valid License (Expires 2009-03-11)	
AV Definitions	8.836 (Updated 2008-03-12 via <i>Manual Update</i>) [Update]	
Extended set	9.004 (Updated 2008-04-22 via <i>Manual Update</i>)	

Intrusion Protection	Valid License (Expires 2009-03-11)	
IPS Definitions	2.506 (Updated 2008-05-27 via <i>Manual Update</i>) [Update]	

Web Filtering	Valid License (Expires 2009-03-11)	

AntiSpam	Valid License (Expires 2009-03-11)	

Management Service	Unreachable [Update]	

Analysis Service	Expired [Renew] [Update]	

▶ AntiVirus and IPS Options		
▶ Web Filtering and AntiSpam Options		
▶ Management and Analysis Service Options		
Apply		

- 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.
- Real 43
Fortinet FCNSA.v5 Exam
- D. They indicate that the FortiGate unit is in the process of downloading updates from the FortiGuard Distribution Network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 108

A FortiGate 100 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.
- D. The FortiGate unit is in Transparent mode.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 109 CORRECT TEXT

In addition to AntiVirus services, the FortiGuard Subscription Services provide IPS, Web Filtering, and _____ services.

- A.
- B.
- C.
- D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: antispam

QUESTION 110

Caching improves performance by reducing FortiGate unit requests to the FortiGuard server.

Which of the following statements are correct regarding the caching of FortiGuard responses? (Select all that apply.)

- A. Caching is available for web filtering, antispam, and IPS requests.
- B. The cache uses a small portion of the FortiGate system memory.
- C. When the cache is full, the least recently used IP address or URL is deleted from the cache.
- D. An administrator can configure the number of seconds to store information in the cache before the FortiGate unit contacts the FortiGuard server again.
Real 44
Fortinet FCNSA.v5 Exam
- E. The size of the cache will increase to accommodate any number of cached queries.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 111

Which of the following products can be installed on a computer running Windows XP to provide personal firewall protection, antivirus protection, web and mail filtering, spam filtering, and VPN functionality?

- A. FortiGate
- B. FortiAnalyzer
- C. FortiClient
- D. FortiManager
- E. FortiReporter

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 112

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 113

Which of the following Fortinet products can receive updates from the FortiGuard Distribution

Real 45

Fortinet FCNSA.v5 Exam

Network? (Select all that apply.)

- A. FortiGate
- B. FortiClient
- C. FortiMail
- D. FortiAnalyzer

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 114

Which Fortinet products & features could be considered part of a comprehensive solution to monitor and prevent the leakage of sensitive data? (Select all that apply.)

- A. Archive non-compliant outgoing e-mails using FortiMail.
- B. Restrict unofficial methods of transferring files such as P2P using Application Control lists on a FortiGate.
- C. Monitor database activity using FortiAnalyzer.
- D. Apply a DLP sensor to a firewall policy.
- E. Configure FortiClient to prevent files flagged as sensitive from being copied to a USB disk.

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 115

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.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Real 46

Fortinet FCNSA.v5 Exam

QUESTION 116

An administrator configures a FortiGate unit in Transparent mode on the 192.168.11.0 subnet. Automatic Discovery is enabled to detect any available FortiAnalyzers on the network.

Which of the following FortiAnalyzers will be detected? (Select all that apply.)

- A. 192.168.11.100
- B. 192.168.11.251
- C. 192.168.10.100
- D. 192.168.10.251

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 117

Which of the following items does NOT support the Logging feature?

- A. File Filter
- B. Application control
- C. Session timeouts
- D. Administrator activities
- E. Web URL filtering

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 118

DLP archiving gives the ability to store session transaction data on 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
- Real 47
Fortinet FCNSA.v5 Exam

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 119

Alert emails enable the FortiGate unit to send email notifications to an email address upon detection of a pre-defined event type. Which of the following are some of the available event types in Web Config? (Select all that apply.)

- A. Intrusion detected.
- B. Successful firewall authentication.
- C. Oversized file detected.
- D. DHCP address assigned.
- E. FortiGuard Web Filtering rating error detected.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Real 48