Fortinet FCNSA.v5 Exam Questions & Answers

Number: FCNSA.v5
Passing Score: 500
Time Limit: 60 min
File Version: 25.4

Fortinet FCNSA.v5 Exam Questions & Answers

Exam Name: Fortinet Certified Network Security Administrator (FCNSA.v5)

For Full Set of Questions please visit: http://www.actualanswers.com/newexams/FCNSA-v5.htm

Actualanswers

QUESTION 1
Which of the following are valid authentication user group types on a FortiGate unit? (Select all that apply.)

A. Firewall
B. Active Directory
C. Local
D. SSL VPN
E. PKI

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
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 accessing 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:

QUESTION 4
Which of the following items represent the minimum configuration steps an administrator must perform to enable Data Leak Prevention from 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 dip command in the CU.
D. Define one or more DLP rules.
E. Define a DLP sensor.
F. Apply a DLP sensor to a DoS sensor policy.

Correct Answer: ABDE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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.
B. Hard Drive.
C. Gigabit network interfaces.
D. Serial console pat.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
In which order are firewall policies processed on the FortiGate unit?

A. They are processed from the top to 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:

QUESTION 7
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.
F. HTTP
G. FTP

Correct Answer: ABCFG
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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:

QUESTION 10
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: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 meter '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:

QUESTION 12
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:

QUESTION 13
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 causes a host route to be added to the FcrOGate routing table.
C. A route back to the client is automatically created on the FortiGate to match the SSLVPN IP pool from which the IP address assignment was made.
D. The FortiGate adds a route based upon the destination address in the SSL VPN firewall policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Before 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: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which of the following logging options are supported on a FortiGate unit? (Select all that apply.)

A. LDAP
B. Syslog
C. FortiAnalyzer
D. Local

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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:

QUESTION 17
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 Conflg.
C. By using an SSH connection.
D. By using a Telnet connection.

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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. Email quarantine.
D. Banned word.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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:

QUESTION 20
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. Mentor 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: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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:

QUESTION 22
The command structure of the FortiGate CLI consists of commands, objects, branches, tables and parameters.
Within this structure, 'user' would be considered to be which type of item?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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?

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:

QUESTION 24
A FortiAnalyzer device takes advantage of 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:

QUESTION 25

The attached diagram displays the FortiGuard tab in the Web Config. What is meant by a green-colored indicators next to the different FortiGuard Distribution Network services?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: