Vendor: Fortinet

Exam Code:FCNSP

Exam Name: FortiOS 4.0 GA, FortiAnalyzer 4.0 GA(FCNSP v4.0)

Version: Demo

QUESTION 1

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

A. VDOMs divide a single FortiGate unit into two or more virtual units that function as multiple, independent units.

B. A management VDOM handles SNMP, logging, alert email, and FDN-based updates.

C. VDOMs share firmware versions, as well as antivirus and IPS databases.

D. Only administrative users with a \\'super_admin\\' profile will be able to enter multiple VDOMs to make configuration changes.

Correct Answer: ABC

QUESTION 2

A network administrator needs to implement dynamic route redundancy between a FortiGate unit located in a remote office and a FortiGate unit located in the central office.

The remote office accesses central resources using IPSec VPN tunnels through two different Internet providers.

What is the best method for allowing the remote office access to the resources through the FortiGate unit used at the central office?

A. Use two or more route-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.

B. Use two or more policy-based IPSec VPN tunnels and enable OSPF on the IPSec virtual interfaces.

C. Use route-based VPNs on the central office FortiGate unit to advertise routes with a dynamic routing protocol and use a policy-based VPN on the remote office with two or more static default routes.

D. Dynamic routing protocols cannot be used over IPSec VPN tunnels.

Correct Answer: A

QUESTION 3

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

A. Using a hub and spoke topology is required to achieve full redundancy.

B. Using a hub and spoke topology simplifies configuration.

C. Using a hub and spoke topology provides stronger encryption.

D. Using a hub and spoke topology reduces the number of tunnels.

Correct Answer: BD

QUESTION 4

Which of the following statements is correct regarding the antivirus scanning function on the FortiGate unit?

A. Antivirus scanning provides end-to-end virus protection for client workstations.

B. Antivirus scanning provides virus protection for the HTTP, Telnet, SMTP, and FTP protocols.

C. Antivirus scanning supports banned word checking.

D. Antivirus scanning supports grayware protection.

Correct Answer: D

QUESTION 5

Review the IPsec Phase2 configuration shown in the Exhibit; then answer the question following it.

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

A. The Phase 2 will re-key even if there is no traffic.

B. There will be a DH exchange for each re-key.

C. The sequence number of ESP packets received from the peer will not be checked.

D. Quick mode selectors will default to those used in the firewall policy.

Correct Answer: AB

QUESTION 6

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

QUESTION 7

An administrator configures a VPN and selects the Enable IPSec Interface Mode option in the phase 1 settings.

Which of the following statements are correct regarding the IPSec VPN configuration?

A. To complete the VPN configuration, the administrator must manually create a virtual IPSec interface in Web Config under System > Network.

B. The virtual IPSec interface is automatically created after the phase1 configuration.

C. The IPSec policies must be placed at the top of the list.

D. This VPN cannot be used as part of a hub and spoke topology.

E. Routes were automatically created based on the address objects in the firewall policies.

Correct Answer: B

QUESTION 8

Examine the following log message for IPS and identify the valid responses below. (Select all that apply.)

2012-07-01 09:54:28 oid=2 log_id=18433 type=ips subtype=anomaly pri=alert vd=root severity="critical" src="192.168.3.168" dst="192.168.3.170" src_int="port2" serial=0 status="detected" proto=1 service="icmp" count=1 attack_name="icmp_flood" icmp_id="0xa8a4" icmp_type="0x08" icmp_code="0x00" attack_id=16777316 sensor="1" ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 > threshold 50"

A. The target is 192.168.3.168.

B. The target is 192.168.3.170.

C. The attack was detected and blocked.

D. The attack was detected only.

E. The attack was TCP based.

Correct Answer: BD

QUESTION 9

Which of the following DLP actions will always be performed if it is selected?

A. Archive

B. Quarantine Interface

C. Ban Sender

D. Block

E. None

F. Ban

G. Quarantine IP Address

Correct Answer: A

QUESTION 10

When the SSL proxy inspects the server certificate for Web Filtering only in SSL Handshake mode, which certificate field is being used to determine the site rating?

A. Common Name

B. Organization

C. Organizational Unit

D. Serial Number

E. Validity

Correct Answer: A

QUESTION 11

Which of the following describes the difference between the ban and quarantine actions?

A. A ban action prevents future transactions using the same protocol which triggered the ban. A qarantine action blocks all future transactions, regardless of the protocol.

B. A ban action blocks the transaction. A quarantine action archives the data.

C. A ban action has a finite duration. A quarantine action must be removed by an administrator.

D. A ban action is used for known users. A quarantine action is used for unknown users.

Correct Answer: A

QUESTION 12

A static route is configured for a FortiGate unit from the CLI using the following commands:

config router static edit 1 set device "wan1" set distance 20 set gateway 192.168.100.1 next end

Which of the following conditions is NOT required for this static default route to be displayed in the FortiGate unit\\'s routing table?

A. The Administrative Status of the wan1 interface is displayed as Up.

B. The Link Status of the wan1 interface is displayed as Up.

C. All other default routes should have an equal or higher distance.

D. You must disable DHCP client on that interface.

Correct Answer: D

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase
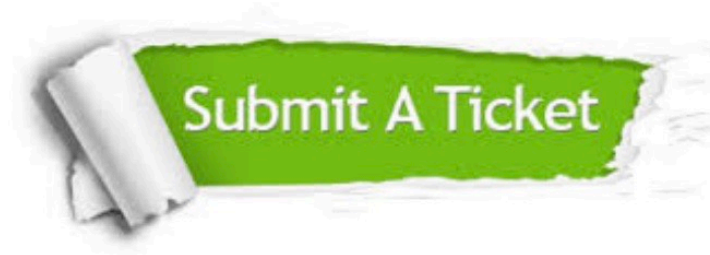
24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

One Year Free Update
Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.

Money Back Guarantee
To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.

Security & Privacy
We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.