

NSE4-5.4

Number: NSE4-5.4
Passing Score: 800
Time Limit: 120 min
File Version: 1.0



VCE to PDF Converter : <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

Google+ : <https://plus.google.com/+Vcepluscom>

LinkedIn : <https://www.linkedin.com/company/vceplus>

<https://vceplus.com/>

NSE4-5.4

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Exam A

QUESTION 1

A FortiGate interface is configured with the following commands:

```
config system interface
edit "port1"
config ipv6
set ip6-address 2001:db8:1::254/64
set ip6-send-adv enable
config ip6-prefix-list
edit 2001:db8:1::/64
set autonomous-flag enable
set onlink-flag enable
end
```

What statements about the configuration are correct? (Choose two.)

- A. IPv6 clients connected to `port1` can use SLAAC to generate their IPv6 addresses.
- B. FortiGate can provide DNS settings to IPv6 clients.
- C. FortiGate can send IPv6 router advertisements (RAs.)
- D. FortiGate can provide IPv6 addresses to DHCPv6 client.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

Which of the following Fortinet hardware accelerators can be used to offload flow-based antivirus inspection? (Choose two.)

- A. SP3



<https://vceplus.com/>

- B. CP8
- C. NP4
- D. NP6

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

Under what circumstance would you enable **LEARN** as the **Action** on a firewall policy?

- A. You want FortiGate to compile security feature activity from various security-related logs, such as virus and attack logs.
- B. You want FortiGate to monitor a specific security profile in a firewall policy, and provide recommendations for that profile.
- C. You want to capture data across all traffic and security vectors, and receive learning logs and a report with recommendations.
- D. You want FortiGate to automatically modify your firewall policies as it learns your networking behavior.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

What methods can be used to deliver the token code to a user who is configured to use two-factor authentication? (Choose three.)

- A. Code blocks

- B. SMS phone message
- C. FortiToken
- D. Browser pop-up window
- E. Email

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

You are tasked to architect a new IPsec deployment with the following criteria:

- There are two HQ sites that all satellite offices must connect to.
- The satellite offices do not need to communicate directly with other satellite offices.
- No dynamic routing will be used.
- The design should minimize the number of tunnels being configured.

Which topology should be used to satisfy all of the requirements?

- A. Redundant
- B. Hub-and-spoke
- C. Partial mesh
- D. Fully meshed

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

View the exhibit.

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Device	TunnelB		
Administrative Distance	5		
Comments			
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<input checked="" type="checkbox"/> Advanced Options			
Priority	30		

Destination	Subnet	Named Address	Internet Service
	172.13.24.0/255.255.255.0		
Device	TunnelA		
Administrative Distance	10		
Comments			
Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled		
<input checked="" type="checkbox"/> Advanced Options			
Priority	0		

Which of the following statements are correct? (Choose two.)

- A. This is a redundant IPsec setup.
- B. The **TunnelB** route is the primary one for searching the remote site. The **TunnelA** route is used only if the **TunnelB** VPN is down.
- C. This setup requires at least two firewall policies with action set to IPsec.
- D. Dead peer detection must be disabled to support this type of IPsec setup.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

Which statements about DNS filter profiles are true? (Choose two.)

- A. They can inspect HTTP traffic.
- B. They must be applied in firewall policies with SSL inspection enabled.
- C. They can block DNS request to known botnet command and control servers.
- D. They can redirect blocked requests to a specific portal.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 8

An administrator needs to offload logging to FortiAnalyzer from a FortiGate with an internal hard drive. Which statements are true? (Choose two.)



<https://vceplus.com/>

- A. Logs must be stored on FortiGate first, before transmitting to FortiAnalyzer
- B. FortiGate uses port 8080 for log transmission
- C. Log messages are transmitted as plain text in LZ4 compressed format (store-and-upload method).
- D. FortiGate can encrypt communications using SSL encrypted OFTP traffic.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

Which of the following statements describe WMI polling mode for FSSO collector agent? (Choose two.)

- A. The collector agent does not need to search any security event logs.
- B. WMI polling can increase bandwidth usage with large networks.
- C. The **NetSessionEnum** function is used to track user logoffs.
- D. The collector agent uses a Windows API to query DCs for user logins.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

An administrator observes that the `port1` interface cannot be configured with an IP address. What can be the reasons for that? (Choose three.)

- A. The interface has been configured for one-arm sniffer.
- B. The interface is a member of a virtual wire pair.
- C. The operation mode is transparent.
- D. The interface is a member of a zone.
- E. Captive portal is enabled in the interface.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

View the example routing table.

```
s* 0.0.0.0/0 [10/0] via 172.20.121.2, port1
C 172.20.121.0/24 is directly connected, port1
C 172.20.168.0/24 is directly connected, port2
C 172.20.167.0/24 is directly connected, port3
S 10.20.30.0/26 [10/0] via 172.20.168.254, port2
S 10.20.30.0/24 [10/0] via 172.20.167.254, port3
```

Which route will be selected when trying to reach 10.20.30.254?

- A. 10.20.30.0/26 [10/0] via 172.20.168.254, port2
- B. The traffic will be dropped because it cannot be routed.
- C. 10.20.30.0/24 [10/0] via 172.20.167.254, port3
- D. 0.0.0.0/0 [10/0] via 172.20.121.2, port1

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 12

When browsing to an internal web server using a web-mode SSL VPN bookmark, which IP address is used as the source of the HTTP request?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 13

What is FortiGate's behavior when local disk logging is disabled?

- A. Only real-time logs appear on the FortiGate dashboard.
- B. No logs are generated.
- C. Alert emails are disabled.
- D. Remote logging is automatically enabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

What traffic and attacks can be blocked by a web application firewall (WAF) profile? (Choose three.)

- A. Traffic to inappropriate web sites
- B. SQL injection attacks
- C. Server information disclosure attacks
- D. Credit card data leaks
- E. Traffic to botnet command and control (C&C) servers



Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

Which statements about **One-to-One** IP pool are true? (Choose two.)

- A. It allows configuration of ARP replies.
- B. It allows fixed mapping of an internal address range to an external address range.
- C. It is used for destination NAT.

D. It does not use port address translation.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Which statements correctly describe transparent mode operation? (Choose three.)

- A. All interfaces of the transparent mode FortiGate device must be on different IP subnets.
- B. The transparent FortiGate is visible to network hosts in an IP traceroute.
- C. It permits inline traffic inspection and firewalling without changing the IP scheme of the network.



<https://vceplus.com/>

- D. Ethernet packets are forwarded based on destination MAC addresses, not IP addresses.
- E. The FortiGate acts as transparent bridge and forwards traffic at Layer-2.

Correct Answer: CDE

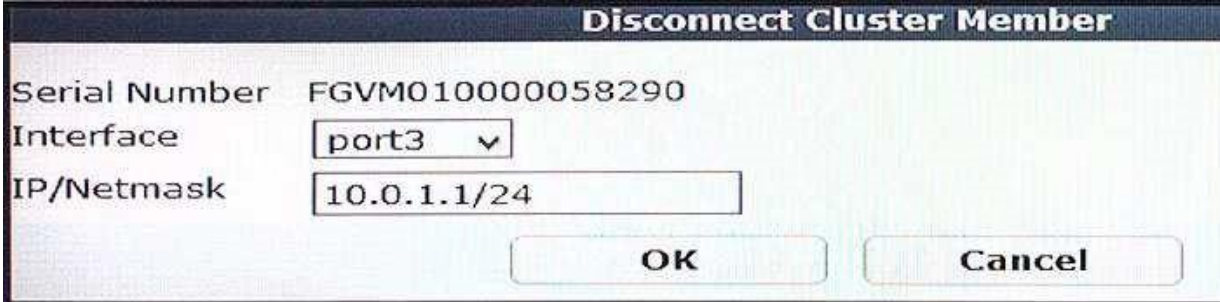
Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

View the exhibit.



Disconnect Cluster Member

Serial Number FGVM010000058290

Interface

IP/Netmask

What is the effect of the **Disconnect Cluster Member** operation as shown in the exhibit? (Choose two.)

- A. The HA mode changes to standalone.
- B. The firewall policies are deleted on the disconnected member.
- C. The system hostname is set to the FortiGate serial number.
- D. The port3 is configured with an IP address for management access.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

What step is required an SSL VPN to access to an internal server using port forward mode?

- A. Configure the virtual IP addresses to be assigned to the SSL VPN users.
- B. Install FortiClient SSL VPN client
- C. Create a SSL VPN realm reserved for clients using port forward mode.
- D. Configure the client application to forward IP traffic to a Java applet proxy.

Correct Answer: D

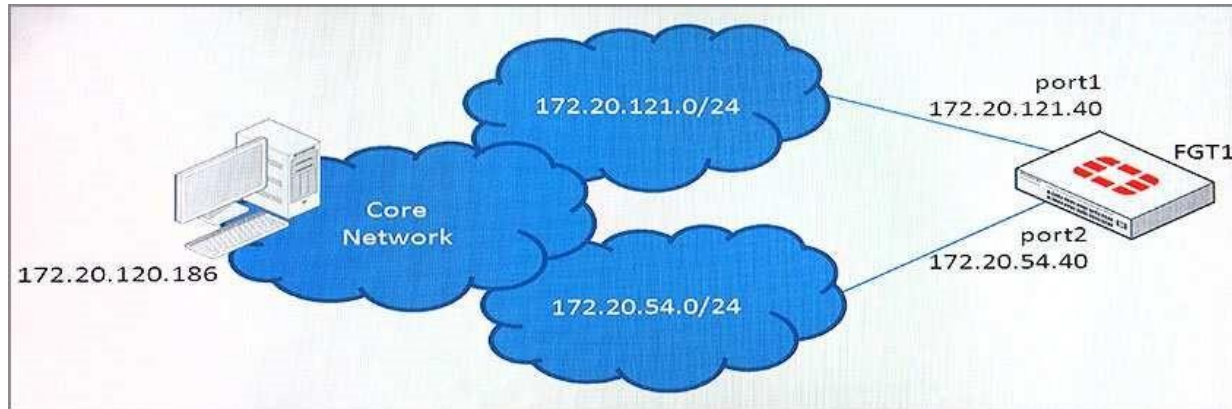
Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

View the exhibit.



This is a sniffer output of a telnet connection request from 172.20.120.186 to the port1 interface of FGT1.

```

FGT1 # di sniff pack any "host 172.20.120.186 and port 23" 4
4.571724 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
7.575327 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
9.571446 port1 in 172.20.120.186.60584 -> 172.20.121.40.23: syn 273086
  
```

In this scenario, FGT1 has the following routing table:

```

S*  0.0.0.0/0 [10/0] via 172.20.54.254, port2
C    172.20.54.0/24 is directly connected, port2
C    172.20.121.0/24 is directly connected, port1
  
```

Assuming telnet service is enabled for port1, which of the following statements correctly describes why FGT1 is not responding?

- A. The port1 cable is disconnected.
- B. The connection is dropped due to reverse path forwarding check.
- C. The connection is denied due to forward policy check.
- D. FGT1's port1 interface is administratively down.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

An administrator needs to be able to view logs for application usage on your network. What configurations are required to ensure that FortiGate generates logs for application usage activity? (Choose two.)

- A. Enable a web filtering profile on the firewall policy.
- B. Create an application control policy.
- C. Enable logging on the firewall policy.
- D. Enable an application control security profile on the firewall policy.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:



QUESTION 21

A company needs to provide SSL VPN access to two user groups. The company also needs to display different welcome messages on the SSL VPN login screen for both user groups.

What is required in the SSL VPN configuration to meet these requirements?

- A. Two separated SSL VPNs in different interfaces of the same VDOM
- B. Different SSL VPN realms for each group
- C. Different virtual SSLVPN IP addresses for each group
- D. Two firewall policies with different captive portals

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:**QUESTION 22**

Examine the routing database.

```
S    *> 0.0.0.0/0 [10/0] via 172.20.121.2, port1, [20/0]
      *>                [10/0] via 10.0.0.2, port2, [30/0]
S    0.0.0.0/0 [20/0] via 192.168.15.2, port3, [10/0]
C    *> 10.0.0.0/24 is directly connected, port2
S    172.13.24.0/24 [10/0] is directly connected, port4
C    *> 172.20.121.0/24 is directly connected, port1
S    *> 192.167.1.0/24 [10/0] via 10.0.0.2, port2
C    *> 192.168.15.0/24 is directly connected, port3
```

Which of the following statements are correct? (Choose two.)

- A. The port3 default route has the lowest metric, making it the best route.
- B. There will be eight routes active in the routing table.
- C. The port3 default has a higher distance than the port1 and port2 default routes.
- D. Both port1 and port2 default routers are active in the routing table.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 23

View the exhibit.



When a user attempts to connect to an HTTPS site, what is the expected result with this configuration?

- A. The user is required to authenticate before accessing sites with untrusted SSL certificates.
- B. The user is presented with certificate warnings when connecting to sites that have untrusted SSL certificates.
- C. The user is allowed access all sites with untrusted SSL certificates, without certificate warnings.
- D. The user is blocked from connecting to sites that have untrusted SSL certificates (no exception provided).

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

View the exhibit.

Edit Interface

Interface Name	port1 (00:0C:29:29:38:DA)
Alias	<input type="text"/>
Link Status	Up
Type	Physical Interface
Virtual Domain	root
Role	Undefined

When **Role** is set to **Undefined**, which statement is true?

- A. The GUI provides all the configuration options available for the **port1** interface.
- B. You cannot configure a static IP address for the **port1** interface because it allows only DHCP addressing mode.
- C. Firewall policies can be created from only the **port1** interface to **any** interface.
- D. The **port1** interface is reserved for management only.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

Which statement is true regarding the policy ID numbers of firewall policies?

- A. Change when firewall policies are re-ordered.
- B. Defined the order in which rules are processed.
- C. Are required to modify a firewall policy from the CLI.
- D. Represent the number of objects used in the firewall policy.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

An administrator needs to inspect all web traffic (including Internet web traffic) coming from users connecting to SSL VPN. How can this be achieved?

- A. Disabling split tunneling
- B. Configuring web bookmarks
- C. Assigning public IP addresses to SSL VPN clients
- D. Using web-only mode

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

Which traffic inspection features can be executed by a security processor (SP)? (Choose three.)

- A. TCP SYN proxy
- B. SIP session helper
- C. Proxy-based antivirus
- D. Attack signature matching
- E. Flow-based web filtering



<https://vceplus.com/>

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

An administrator has configured two VLAN interfaces:

```
config system interface
  edit "VLAN10"
    set vdom "VDM1"
    set forward-domain 100
    set role lan
    set interface "port9"
    set vlanid 10
  next
  edit "VLAN5"
    set vdom "VDM1"
    set forward-domain 50
    set role lan
    set interface "port10"
    set vlanid 5
  next
end
```



A DHCP server is connected to the VLAN10 interface. A DHCP client is connected to the VLAN5 interface. However, the DHCP client cannot get a dynamic IP address from the DHCP server. What is the cause of the problem?

- A. Both interfaces must be in different VDOMs
- B. Both interfaces must have the same VLAN ID.
- C. The `role` of the VLAN10 interface must be set to `server`.
- D. Both interfaces must belong to the same forward domain.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

View the exhibit.

Application Details

Name	Category	Technology	Popularity	Risk
Addicting Games	Game	Browser-Based	☆☆☆☆	Low

Application Control Profile

Categories

Botnet	Game	Proxy	Video/Audio
Business	General Interest	Remote Access	VoIP
Cloud.IT	Mobile	Social Media	Web.Client
Collaboration	Network Service	Storage.Backup	Unknown Applications
Email	P2P	Update	

Application Overrides

+ Add Signatures Edit Parameters Delete

Application Signature	Category	Action
Addicting Games	Game	Monitor

Filter Overrides

+ Add Filter Edit Delete

Filter Details	Action
Risk: (Low)	Block

A user behind the FortiGate is trying to go to `http://www.addictinggames.com` (**Addicting.Games**). Based on this configuration, which statement is true?

- A. **Addicting.Games** is allowed based on the **Application Overrides** configuration.
- B. **Addicting.Games** is blocked based on the **Filter Overrides** configuration.
- C. **Addicting.Games** can be allowed only if the **Filter Overrides** actions is set to **Exempt**.
- D. **Addicting.Games** is allowed based on the **Categories** configuration.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

What are the purposes of NAT traversal in IPsec? (Choose two.)

- A. To detect intermediary NAT devices in the tunnel path.
- B. To encapsulate ESP packets in UDP packets using port 4500.
- C. To force a new DH exchange with each phase 2 re-key
- D. To dynamically change phase 1 negotiation mode to Aggressive.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Which statements about application control are true? (Choose two.)

- A. Enabling application control profile in a security profile enables application control for all the traffic flowing through the FortiGate.
- B. It cannot take an action on unknown applications.
- C. It can inspect encrypted traffic.
- D. It can identify traffic from known applications, even when they are using non-standard TCP/UDP ports.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

What FortiGate feature can be used to allow IPv6 clients to connect to IPv4 servers?

- A. IPv6-over-IPv4 IPsec
- B. NAT64
- C. IPv4-over-IPv6 IPsec
- D. NAT66

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 33

Which statements best describe auto discovery VPN (ADVPN). (Choose two.)

- A. It requires the use of dynamic routing protocols so that spokes can learn the routes to other spokes.
- B. ADVPN is only supported with IKEv2.
- C. Tunnels are negotiated dynamically between spokes.
- D. Every spoke requires a static tunnel to be configured to other spokes so that phase 1 and phase 2 proposals are defined in advance.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

View the exhibit.

Status	Name	VLAN ID	Type	IP/Netmask
Physical (12)				
	port1		Physical Interface	10.200.1.1 255.255.255.0
	port1-VLAN1	1	VLAN	10.200.5.1 255.255.255.0
	port1-VLAN10	10	VLAN	10.0.10.1 255.255.255.0
	port2		Physical Interface	10.200.2.1 255.255.255.0
	port2-VLAN1	1	VLAN	10.0.5.1 255.255.255.0
	port2-VLAN10	10	VLAN	10.0.20.254 255.255.255.0
	port3		Physical Interface	10.0.1.254 255.255.255.0

Which statements about the exhibit are true? (Choose two.)

- A. **port1-VLAN10** and **port2-VLAN10** can be assigned to different VDOMs.
- B. **port1-VLAN1** is the native VLAN for the **port1** physical interface.
- C. Traffic between **port1-VLAN1** and **port2-VLAN1** is allowed by default.
- D. Broadcast traffic received in **port1-VLAN10** will not be forwarded to **port2-VLAN10**.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 35

Which statement about the firewall policy authentication timeout is true?

- A. It is a hard timeout. The FortiGate removes the temporary policy for a user's source IP address after this times expires.
- B. It is a hard timeout. The FortiGate removes the temporary policy for a user's source MAC address after this times expires.
- C. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user's source MAC address.
- D. It is an idle timeout. The FortiGate considers a user to be idle if it does not see any packets coming from the user's source IP.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:**QUESTION 36**

Which of the following settings and protocols can be used to provide secure and restrictive administrative access to FortiGate? (Choose three.)

- A. Trusted host
- B. HTTPS
- C. Trusted authentication
- D. SSH
- E. FortiTelemetry

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

If traffic matches a DLP filter with the action set to **Quarantine IP Address**, what action does the FortiGate take?



<https://vceplus.com/>

- A. It blocks all future traffic for that IP address for a configured interval.
- B. It archives the data for that IP address.
- C. It provides a DLP block replacement page with a link to download the file.
- D. It notifies the administrator by sending an email.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

How can a browser trust a web-server certificate signed by a third party CA?

- A. The browser must have the CA certificate that signed the web-server certificate installed.
- B. The browser must have the web-server certificate installed.
- C. The browser must have the private key of CA certificate that signed the web-browser certificate installed.
- D. The browser must have the public key of the web-server certificate installed.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

How does FortiGate verify the login credentials of a remote LDAP user?

- A. FortiGate sends the user entered credentials to the LDAP server for authentication.
- B. FortiGate re-generates the algorithm based on the login credentials and compares it against the algorithm stored on the LDAP server.
- C. FortiGate queries its own database for credentials.
- D. FortiGate queries the LDAP server for credentials.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

An administrator has enabled proxy-based antivirus scanning and configured the following settings:


```
config firewall profile-protocol-options
edit default
config http
set oversize-limit 10
set options oversize
end
end
```

Which statement about the above configuration is true?

- A. Files bigger than 10 MB are not scanned for viruses and will be blocked.
- B. FortiGate scans only the first 10 MB of any file.
- C. Files bigger than 10 MB are sent to the heuristics engine for scanning.
- D. FortiGate scans the files in chunks of 10 MB.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 41

Examine this output from the `diagnose sys top` command:

```
# diagnose sys top 1
Run Time: 11 days, 3 hours and 29 minutes
ON, ON, 1S, 99I; 971T, 528F, 160KF
  sshd          123      S      1.9      1.2
  ipsengine     61       S <      0.0      5.2
  miglogd       45       S      0.0      4.9
  pyfcgid       75       S      0.0      4.5
  pyfcgid       73       S      0.0      3.9
```

Which statements about the output are true? (Choose two.)

- A. `sshd` is the process consuming most memory
- B. `sshd` is the process consuming most CPU
- C. All the processes listed are in sleeping state
- D. The `sshd` process is using 123 pages of memory

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

An administrator has created a custom IPS signature. Where does the custom IPS signature have to be applied?

- A. In an IPS sensor
- B. In an interface.
- C. In a DoS policy.
- D. In an application control profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

An administrator wants to configure a FortiGate as a DNS server. The FortiGate must use its DNS database first, and then relay all irresolvable queries to an external DNS server. Which of the following DNS method must you use?

- A. Non-recursive
- B. Recursive
- C. Forward to primary and secondary DNS
- D. Forward to system DNS

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

When using WPAD DNS method, what is the FQDN format that browsers use to query the DNS server?

- A. wpad.<local-domain>
- B. srv_tcp.wpad.<local-domain>
- C. srv_proxy.<local-domain>/wpad.dat
- D. proxy.<local-domain>.wpad

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 45

An administrator is using the FortiGate built-in sniffer to capture HTTP traffic between a client and a server, however, the sniffer output shows only the packets related with TCP session setups and disconnections. Why?

- A. The administrator is running the sniffer on the internal interface only.
- B. The filter used in the sniffer matches the traffic only in one direction.
- C. The FortiGate is doing content inspection.
- D. TCP traffic is being offloaded to an NP6.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

Which of the following statements about advanced AD access mode for FSSO collector agent are true? (Choose two.)



<https://vceplus.com/>

- A. It is only supported if DC agents are deployed.
- B. FortiGate can act as an LDAP client configure the group filters.
- C. It supports monitoring of nested groups.
- D. It uses the Windows convention for naming, that is, Domain\Username.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 47**

Which configuration objects can be selected for the **Source** field of a firewall policy? (Choose two.)

- A. FQDN address
- B. IP pool
- C. User or user group
- D. Firewall service

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

Examine the exhibit, which contains a virtual IP and a firewall policy configuration.

Virtual IP

Name

Comments

0/255

Network

Interface WAN (port1)

Type Static NAT

External IP Address/Range 10.200.1.10 - 10.200.1.10

Mapped IP Address/Range 10.0.1.10 - 10.0.1.10

Source Address Filter ☐

Port Forwarding ☐

OK
Cancel

Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT
<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #0070c0; margin-right: 5px;"></div> LAN (port2) - WAN (port1) (1 - 1) </div>							
1	Full Access	all	all	always	ALL	✓ ACCEPT	✓ Enabled
<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: #0070c0; margin-right: 5px;"></div> WAN (port1) - LAN (port2) (2 - 2) </div>							
2	WebServer	all	VIP	always	ALL	✓ ACCEPT	✗ Disabled

The top firewall policy has NAT enabled using outgoing interface address. The second firewall policy configured with a virtual IP (**VIP**) as the destination address.

Which IP address will be used to source NAT the Internet traffic coming from a workstation with the IP address 10.0.1.10/24?

- A. 10.200.1.1
- B. 10.0.1.254
- C. Any available IP address in the **WAN(port1)** subnet 10.200.1.0/24
- D. 10.200.1.10

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

Which statement about data leak prevention (DLP) on a FortiGate is true?

- A. Traffic shaping can be applied to DLP sensors.
- B. It can be applied to a firewall policy in a flow-based VDOM.
- C. Files can be sent to FortiSandbox for detecting DLP threats.
- D. It can archive files and messages.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

Which statements about an IPv6-over-IPv4 IPsec configuration are correct? (Choose two.)

- A. The remote gateway IP must be an IPv6 address.
- B. The source quick mode selector must be an IPv4 address.
- C. The local gateway IP must be an IPv4 address.
- D. The destination quick mode selector must be an IPv6 address.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

Which statements about IP-based explicit proxy authentication are true? (Choose two.)

- A. IP-based authentication is best suited to authenticating users behind a NAT device.
- B. Sessions from the same source address are treated as a single user.
- C. IP-based authentication consumes less FortiGate's memory than session-based authentication.
- D. FortiGate remembers authenticated sessions using browser cookies.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>