

NSE4-5.4.exam.59q

Number: NSE4-5.4
Passing Score: 800
Time Limit: 120 min
File Version: 1



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/>

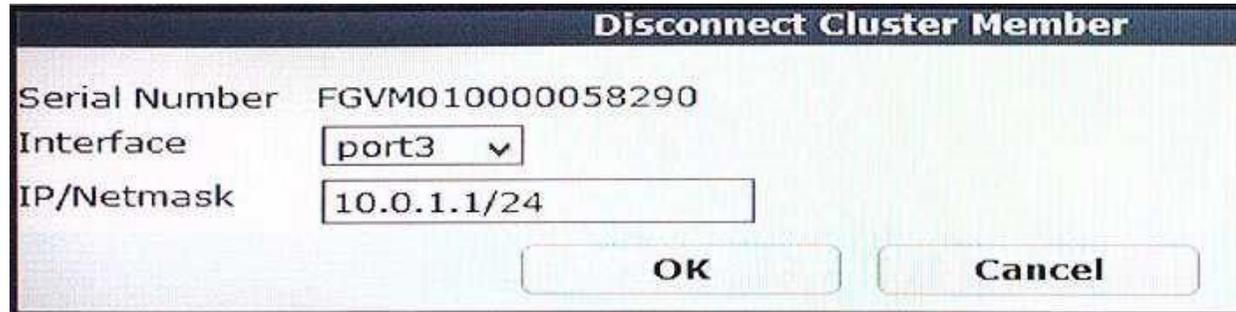
Fortinet NSE4-5.4

Fortinet Network Security Expert 4 Written Exam - FortiOS 5.4

Exam A

QUESTION 1

View the exhibit.



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



<https://vceplus.com/>

- 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 2

What step is required to configure 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

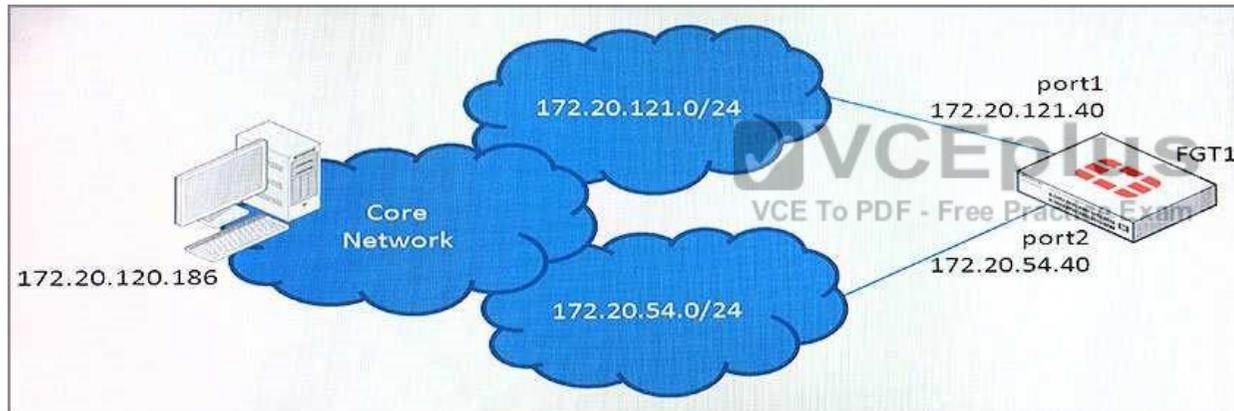
Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

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 4

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 5

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 6

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.)



<https://vceplus.com/> 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: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

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

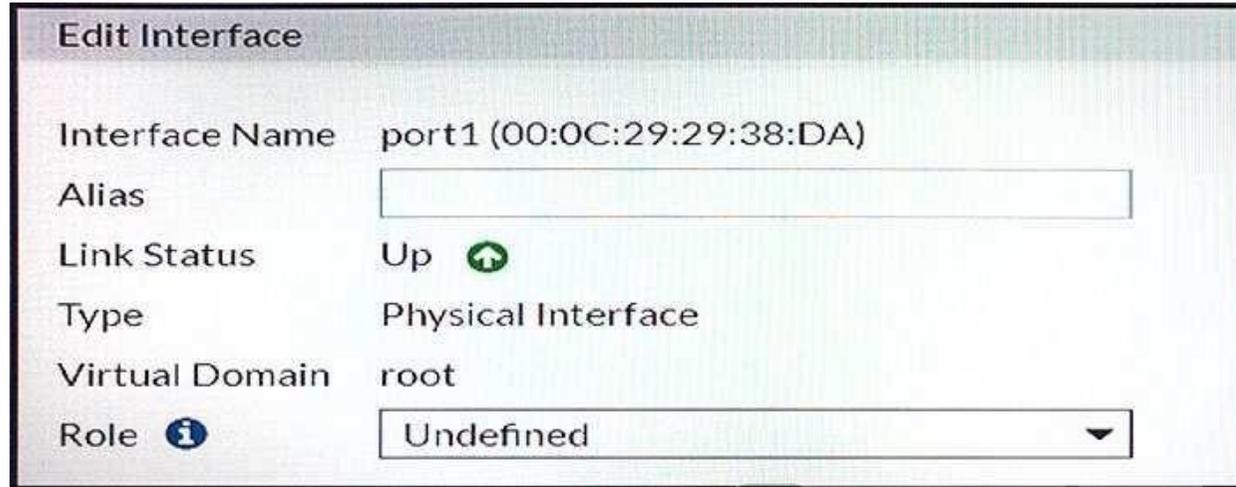
Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

View the exhibit.



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 9

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

- A. Change when firewall policies are re-ordered.

- B. Defines 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 10

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 11

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

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 12

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?



<https://vceplus.com/>

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 13

View the exhibit.

The screenshot shows the 'Application Control Profile' configuration for 'Addicting Games'. The 'Categories' section is expanded to show 'Game' selected. The 'Application Overrides' table shows the application signature 'Addicting Games' with a 'Monitor' action. The 'Filter Overrides' table shows a filter with a 'Block' action.

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

Application Control Profile

Categories

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

Application Overrides

Application Signature	Category	Action
Addicting Games	Game	Monitor

Filter Overrides

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 14

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 15

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

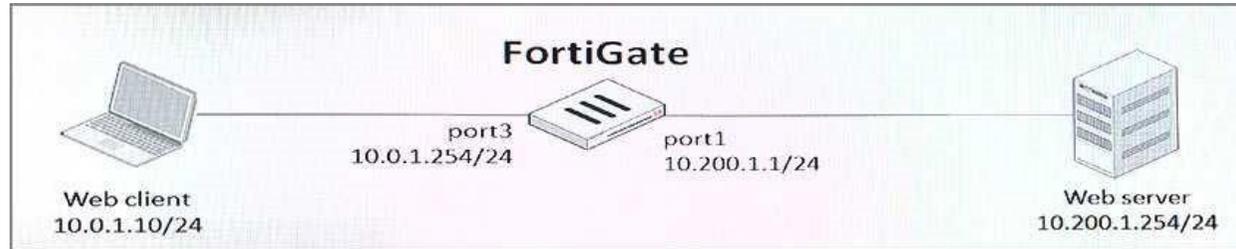
- A. Enabling application control profile in a security profile enables application control for all the traffic flowing through the FortiGate.
- B. It cannot take an action on unknown applications.
- C. It can inspect encrypted traffic.
- D. It can identify traffic from known applications, even when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

Correct Answer: CD

Section: (none)
Explanation

Explanation/Reference:
QUESTION 16

View the exhibit.



The client cannot connect to the HTTP web server. The administrator run the FortiGate built-in sniffer and got the following output:

```
FortiGate # diagnose sniffer packet any "port 80" 4
interfaces=[any]
filters=[port 80]
11.510058 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
11.760531 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
14.505371 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 697263124
14.755510 port3 in 10.0.1.10.49255 -> 10.200.1.254.80: syn 868017830
```

What should be done next to troubleshoot the problem?

- A. Execute another sniffer in the FortiGate, this time with the filter "host 10.0.1.10".
- B. Run a sniffer in the web server.
- C. Capture the traffic using an external sniffer connected to port1.
- D. Execute a debug flow.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

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

- A. It is useful when users log in to DCs that are not monitored by a collector agent.
- B. It takes over as the primary authentication method when configured alongside FSSO.
- C. Multi-domain environments require DC agents on every domain controller.
- D. NTLM-enabled web browsers are required.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

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: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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 20

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 21

Which statement about the firewall policy authentication timeout is true?



<https://vceplus.com/>

- 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 22

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 23

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

- 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 24

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 25

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: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

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 27

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 28

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 29

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 30

Which statements about high availability (HA) for FortiGates are true? (Choose two.)

- A. Virtual clustering can be configured between two FortiGate devices with multiple VDOM.
- B. Heartbeat interfaces are not required on the primary device.
- C. HA management interface settings are synchronized between cluster members.
- D. Sessions handled by UTM proxy cannot be synchronized.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Which of the following statements about central NAT are true? (Choose two.)

- A. IP tool references must be removed from existing firewall policies before enabling central NAT.



<https://vceplus.com/>

- B. Central NAT can be enabled or disabled from the CLI only.
- C. Source NAT, using central NAT, requires at least one central SNAT policy.
- D. Destination NAT, using central NAT, requires a VIP object as the destination address in a firewall policy.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

Which statement about the FortiGuard services for the FortiGate is true?

- A. Antivirus signatures are downloaded locally on the FortiGate.
- B. FortiGate downloads IPS updates using UDP port 53 or 8888.
- C. FortiAnalyzer can be configured as a local FDN to provide antivirus and IPS updates.
- D. The web filtering database is downloaded locally on the FortiGate.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

Which statements about antivirus scanning using flow-based full scan are true? (Choose two.)

- A. The antivirus engine starts scanning a file after the last packet arrives.
- B. It does not support FortiSandbox inspection.

- C. FortiGate can insert the block replacement page during the first connection attempt only if a virus is detected at the start of the TCP stream.
- D. It uses the compact antivirus database.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

An administrator has configured a route-based IPsec VPN between two FortiGates. Which statement about this IPsec VPN configuration is true?

- A. A phase 2 configuration is not required.
- B. This VPN cannot be used as part of a hub and spoke topology.
- C. The IPsec firewall policies must be placed at the top of the list.
- D. A virtual IPsec interface is automatically created after the phase 1 configuration is completed.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 35

What information is flushed when the `chunk-size` value is changed in the `config dlp settings`?

- A. The database for DLP document fingerprinting
- B. The supported file types in the DLP filters
- C. The archived files and messages
- D. The file name patterns in the DLP filters

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 36**

How does FortiGate select the central SNAT policy that is applied to a TCP session?

- A. It selects the SNAT policy specified in the configuration of the outgoing interface.
- B. It selects the first matching central-SNAT policy from top to bottom.
- C. It selects the central-SNAT policy with the lowest priority.
- D. It selects the SNAT policy specified in the configuration of the firewall policy that matches the traffic.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

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 38

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 39

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

- 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: BC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 40

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: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

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

Virtual IP

Name:

Comments:

Network

Interface:

Type: Static NAT

External IP Address/Range: -

Mapped IP Address/Range: -

Source Address Filter:

Port Forwarding:

Firewall Policies

Seq.#	Name	Source	Destination	Schedule	Service	Action	NAT
LAN (port2) - WAN (port1) (1 - 1)							
1	Full Access	all	all	always	ALL	ACCEPT	Enabled
WAN (port1) - LAN (port2) (2 - 2)							
2	WebServer	all	VIP	always	ALL	ACCEPT	Disabled

The **WAN(port1)** interface has the IP address 10.200.1.1/24. The **LAN(port2)** interface has the IP address 10.0.1.254/24.

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.



<https://vceplus.com/>

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: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

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 43

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: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 44

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)

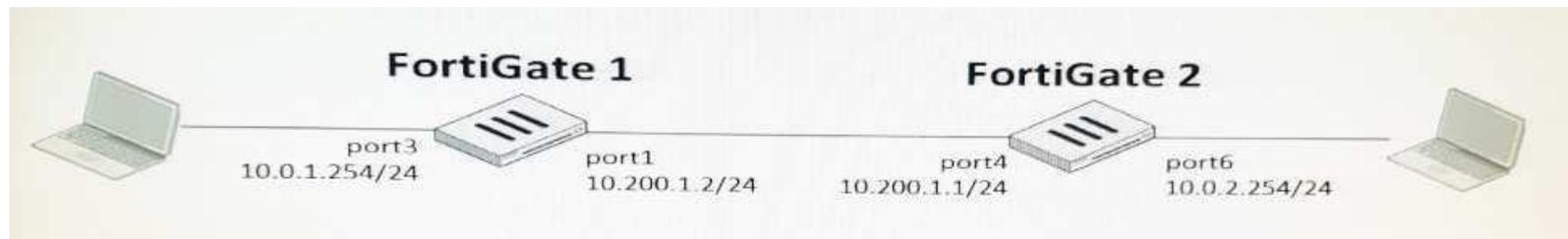
Explanation

Explanation/Reference:



QUESTION 45

View the Exhibit.



The administrator needs to confirm that FortiGate 2 is properly routing that traffic to the 10.0.1.0/24 subnet. The administrator needs to confirm it by sending ICMP pings to FortiGate 2 from the CLI of FortiGate 1. What ping option needs to be enabled before running the ping?

- A. Execute ping-options source port1
- B. Execute ping-options source 10.200.1.1.
- C. Execute ping-options source 10.200.1.2

D. Execute ping-options source 10.0.1.254

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

How can you format the FortiGate flash disk?

- A. Load the hardware test (HQIP) image.
- B. Execute the CLI command execute formatlogdisk.
- C. Load a debug FortiOS image.
- D. Select the format boot device option from the BIOS menu.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 47

How do you configure inline SSL inspection on a firewall policy? (Choose two.)

- A. Enable one or more flow-based security profiles on the firewall policy.
- B. Enable the SSL/SSH Inspection profile on the firewall policy.
- C. Execute the inline ssl inspection CLI command.
- D. Enable one or more proxy-based security profiles on the firewall policy.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

Which traffic sessions can be offloaded to a NP6 processor? (Choose two.)

- A. IPv6
- B. RIP
- C. GRE
- D. NAT64

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

View the exhibit.

```
#diagnose hardware sysinfo shm
```

```
SHM COUNTER:          10316
SHM allocated:        617643792
SHM total:            1572380672
conserve mode:       on-mem
system last entered: Fri Jun 3 10:16:39 2016
sys fd last entered: n/a
SHM FS total:         1607806976
SHM FS free:          990134272
SHM FS avail:         990134272
SHM FS alloc:         617672704
```



Based on this output, which statements are correct? (Choose two.)

- A. FortiGate generated an event log for system conserve mode.

- B. FortiGate has entered in to system conserve mode.
- C. By default, the FortiGate blocks new sessions.
- D. FortiGate changed the global av-failopen settings to idledrop.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

An administrator has blocked Netflix login in a cloud access security inspection (CASl) profile. The administrator has also applied the CASl profile to a firewall policy.

What else is required for the CASl profile to work properly?



<https://vceplus.com/>

- A. You must enable logging for security events on the firewall policy.
- B. You must activate a FortiCloud account.
- C. You must apply an application control profile to the firewall policy.
- D. You must enable SSL inspection on the firewall policy.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

How does FortiGate look for a matching firewall policy to process traffic?

- A. From top to bottom, based on the sequence numbers.
- B. Based on best match.
- C. From top to bottom, based on the policy ID numbers.
- D. From lower to higher, based on the priority value.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

How do you configure a FortiGate to do traffic shaping of P2P traffic, such as BitTorrent?

- A. Apply an application control profile allowing BitTorrent to a firewall policy and configure a traffic shaping policy.
- B. Enable the shape option in a firewall policy with service set to BitTorrent.
- C. Apply a traffic shaper to a BitTorrent entry in the SSL/SSH inspection profile.
- D. Apply a traffic shaper to a protocol options profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

Which file names will match the *.tiff file name pattern configured in a data leak prevention filter? (Choose two.)

- A. tiff.tiff
- B. tiff.png
- C. tiff.jpeg
- D. gif.tiff



<https://vceplus.com/>

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

An administrator has configured the following settings:

```
config system settings
set ses-denied-traffic enable
end
```

```
config system global
set block-session-timer 30
end
```



What does the configuration do? (Choose two.)

- A. Reduces the amount of logs generated by denied traffic.
- B. Enforces device detection on all interfaces for 30 minutes.
- C. Blocks denied users for 30 minutes.
- D. Creates a session for traffic being denied.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

Which statements about FortiGate inspection modes are true? (Choose two.)

- A. The default inspection mode is proxy based.
- B. Switching from proxy-based mode to flow-based, then back to proxy-based mode, will not result in the original configuration.
- C. Proxy-based inspection is not available in VDOMs operating in transparent mode.
- D. Flow-based profiles must be manually converted to proxy-based profiles before changing the inspection mode from flow based to proxy based.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:



QUESTION 56

Examine the following interface configuration on a FortiGate in transparent mode:

```
config system interface
  edit <interface name>
    set stop-forward enable
  end
```

Which statement about this configuration is correct?

- A. The FortiGate generates spanning tree BPDU frames.
- B. The FortiGate device forwards received spanning tree BPDU frames.
- C. The FortiGate can block an interface if a layer-2 loop is detected.
- D. Ethernet layer-2 loops are likely to occur.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

Examine this PAC file configuration.

```
function FindProxyForURL (url, host) {  
  if (shExpMatch (url, "*.fortinet.com/*")) {  
    return "DIRECT";  
  }  
  if (isInNet (host, "172.25.120.0", "255.255.255.0")) {  
    return "PROXY altproxy.corp.com: 8060";  
  }  
  return "PROXY proxy.corp.com: 8090";  
}
```



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

- A. Browsers can be configured to retrieve this PAC file from the FortiGate.
- B. Any web request to the 172.25.120.0/24 subnet is allowed to bypass the proxy.
- C. All requests not made to Fortinet.com or the 172.25.120.0/24 subnet, have to go through altproxy.corp.com: 8060.
- D. Any web request fortinet.com is allowed to bypass the proxy.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 58

In a high availability (HA) cluster operating in active-active mode, which of the following correctly describes the path taken by the SYN packet of an HTTP session that is offloaded to a secondary FortiGate?

- A. Client > primary FortiGate> secondary FortiGate> primary FortiGate> web server.
- B. Client > secondary FortiGate> web server.
- C. Client >secondary FortiGate> primary FortiGate> web server.
- D. Client> primary FortiGate> secondary FortiGate> web server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

A FortiGate is operating in NAT/Route mode and configured with two virtual LAN (VLAN) sub-interfaces added to the same physical interface.

Which statement about the VLAN IDs in this scenario is true?

- A. The two VLAN sub-interfaces can have the same VLAN ID only if they belong to different VDOMs.
- B. The two VLAN sub-interfaces must have different VLAN IDs.
- C. The two VLAN sub-interfaces can have the same VLAN ID only if they have IP addresses in the same subnet.
- D. The two VLAN sub-interfaces can have the same VLAN ID only if they have IP addresses in different subnets.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>