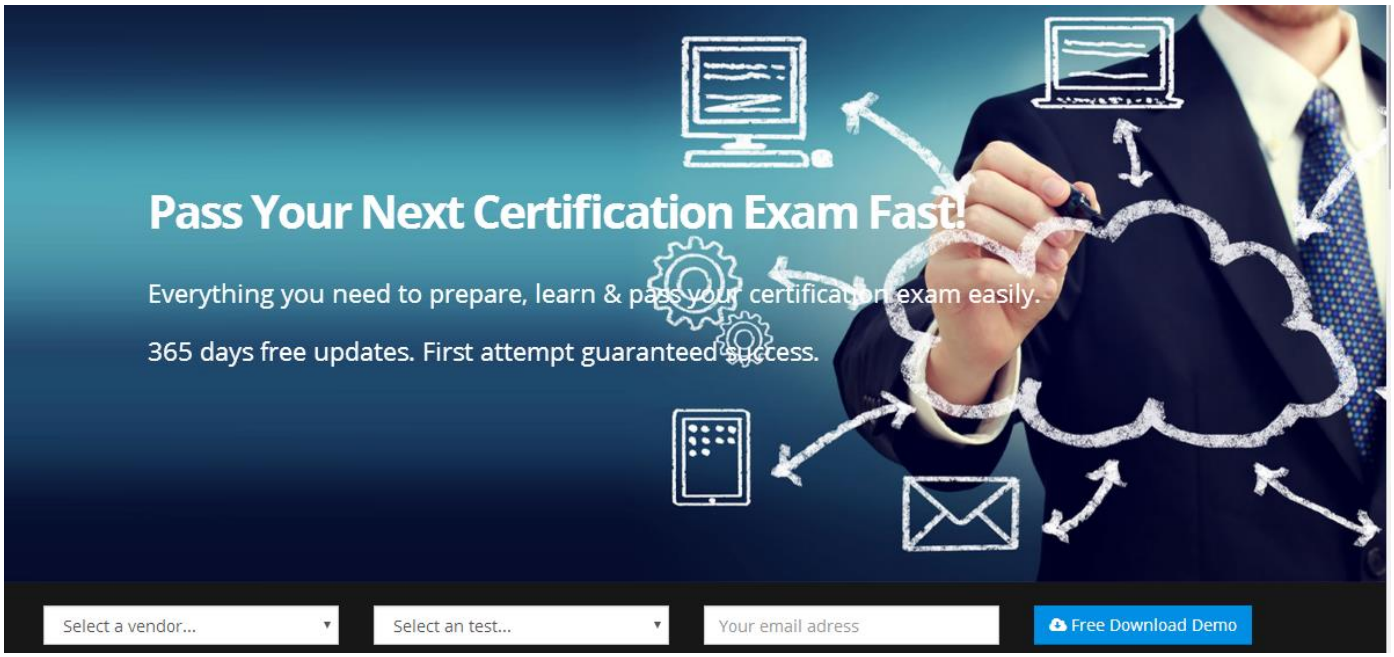
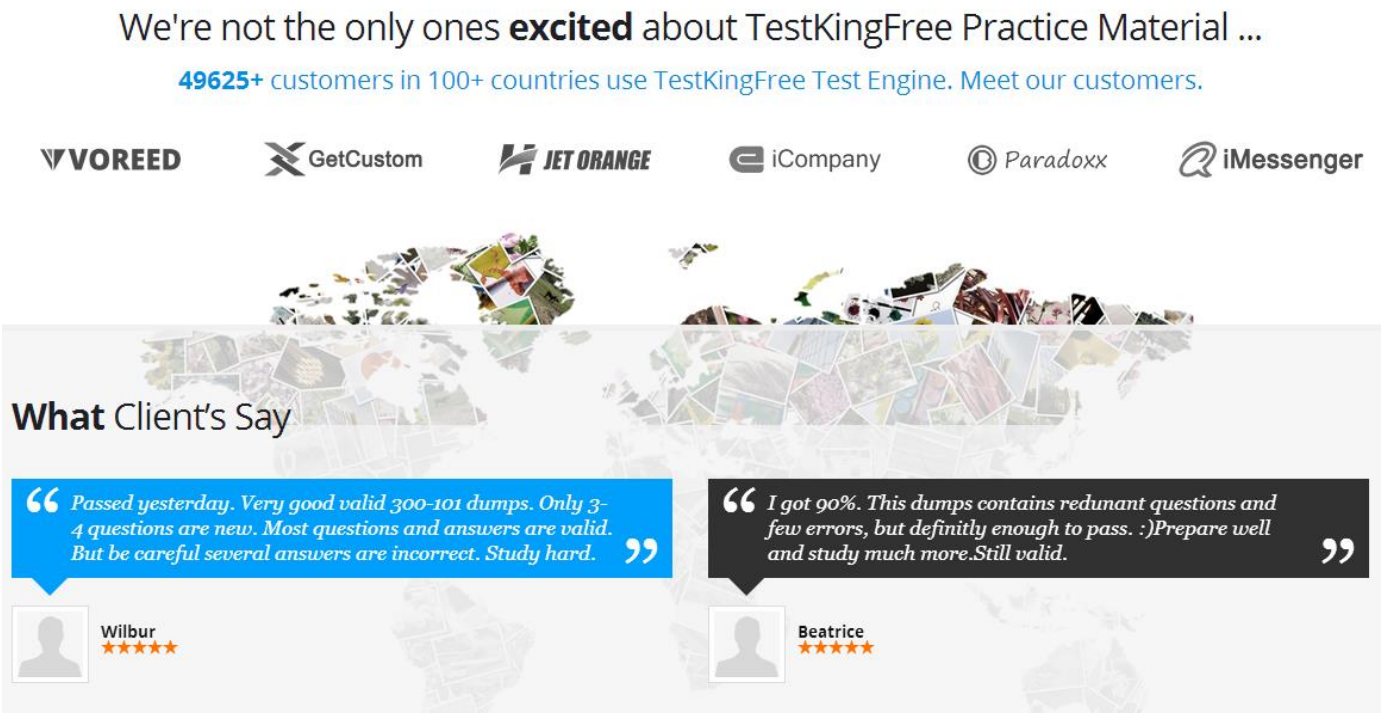
TestKingfree





http://www.testkingfree.com/

Pass For sure Certification Exam Guide and Exam Dumps - TestKingFree

Exam : **FCP_FGT_AD-7.4**

Title : FCP - FortiGate 7.4 Administrator

Vendor : Fortinet

Version : DEMO

NO.1 Refer to the exhibit.

IPS diagnostic output

```
# diagnose test application ipsmonitor

1: Display IPS engine information
2: Toggle IPS engine enable/disable status
3: Display restart log
4: Clear restart log
5: Toggle bypass status
6: Submit attack characteristics now
10: IPS queue length
11: Clear IPS queue length
12: IPS L7 socket statistics
13: IPS session list
14: IPS NTurbo statistics
15: IPSA statistics
...
97: Start all IPS engines
98: Stop all IPS engines
99: Restart all IPS engines and monitor
```

Examine the intrusion prevention system (IPS) diagnostic command shown in the exhibit.
If option 5 is used with the IPS diagnostic command and the outcome is a decrease in the CPU usage, what is the correct conclusion?

A. The IPS engine is blocking all traffic.

B. The IPS engine is inspecting a high volume of traffic.

C. The IPS engine is unable to prevent an intrusion attack.

D. The IPS engine will continue to run in a normal state.

Answer: B

Explanation:
If there are high-CPU use problems caused by the IPS, you can use the diagnose test application ipsmonitor command with option 5 to isolate where the problem might be. Option 5 enables IPS bypass mode. In this mode, the IPS engine is still running, but it is not inspecting traffic. If the CPU use decreases after that, it usually indicates that the volume of traffic being inspected is too high for that FortiGate model.

NO.2 Refer to the exhibits, which show the firewall policy and an antivirus profile configuration.

Why is the user unable to receive a block replacement message when downloading an infected file for the first time?

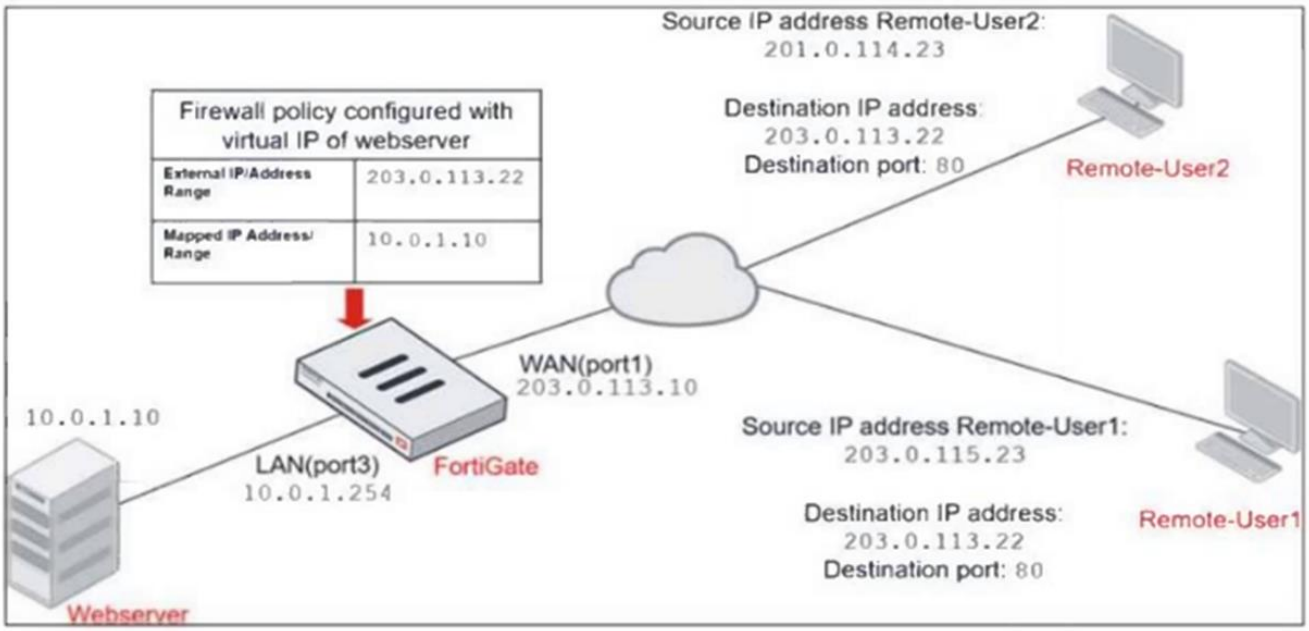
A. The intrusion prevention security profile must be enabled when using flow-based inspection mode.
B. The option to send files to FortiSandbox for inspection is enabled.
C. The firewall policy performs a full content inspection on the file.
D. Flow-based inspection is used, which resets the last packet to the user.
Answer: D
Explanation:
In flow-based inspection mode, FortiGate sends a reset (RST) packet to the client instead of providing a replacement message, which causes the block message not to be displayed.

NO.3 Which two statements about equal-cost multi-path (ECMP) configuration on FortiGate are true? (Choose two.)
A. If SD-WAN is enabled, you control the load balancing algorithm with the parameter load-balance-mode.
B. If SD-WAN is disabled, you can configure the parameter v4-ecmp-mode to volume-based.
C. If SD-WAN is enabled, you can configure routes with unequal distance and priority values to be part of ECMP
D. If SD-WAN is disabled, you configure the load balancing algorithm in config system settings.
Answer: A,D
Explanation:
When SD-WAN is enabled on FortiGate, the load balancing algorithm for Equal-Cost Multi-Path (ECMP) is configured using the load-balance-mode parameter under SD-WAN settings. However, if SD-WAN is disabled, the ECMP load balancing algorithm can be configured under config system settings. This flexibility allows FortiGate to control traffic routing behavior based on the network configuration and requirements.
Reference:
FortiOS 7.4.1 Administration Guide: ECMP Configuration

NO.4 Which two features of IPsec IKEv1 authentication are supported by FortiGate? (Choose two.)
A. Pre-shared key and certificate signature as authentication methods
B. Extended authentication (XAuth)to request the remote peer to provide a username and password
C. Extended authentication (XAuth) for faster authentication because fewer packets are exchanged
D. No certificate is required on the remote peer when you set the certificate signature as the authentication method
Answer: A,B
Explanation:
FortiGate supports both pre-shared key and certificate signature methods for IKEv1 authentication. These methods provide flexibility depending on the security requirements of the network. Additionally, FortiGate supports Extended Authentication (XAuth), which requests a username and password from the remote peer, enhancing security by adding an extra layer of authentication. The XAuth method does not necessarily make the authentication faster; it is an additional security measure.
Reference:
FortiOS 7.4.1 Administration Guide: IPsec VPN Configuration

NO.5 Refer to the exhibits.

Network diagram



Firewall address object

Firewall policies

ID	Name	Source	Destination	Schedule	Service	Action
WAN (port1) → LAN (port3) 2						
4	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Webserver	always	ALL	ACCEPT

The exhibits show a diagram of a FortiGate device connected to the network, and the firewall

configuration.
An administrator created a Deny policy with default settings to deny Webserver access for Remote-User2.
The policy should work such that Remote-User1 must be able to access the Webserver while preventing Remote-User2 from accessing the Webserver.
Which two configuration changes can the administrator make to the policy to deny Webserver access for Remote-User2? (Choose two.)

A. Enable match-vip in the Deny policy.

B. Set the Destination address as Webserver in the Deny policy.

C. Disable match-vip in the Deny policy.

D. Set the Destination address as Deny_IP in the Allow_access policy.

Answer: A,B

Explanation:
To deny access to the web server for Remote-User2 while allowing Remote-User1 to access the same web server, two configuration changes can be made:
Enable match-vip in the Deny policy:
By enabling the match-vip option in the Deny policy, the FortiGate will check for virtual IP (VIP) objects during policy matching. This setting allows the firewall policy to correctly identify and block traffic directed to a specific mapped IP address, such as the web server, when using a VIP configuration.
Set the Destination address as Webserver in the Deny policy:
Setting the Destination address to "Webserver" in the Deny policy ensures that the policy specifically targets traffic attempting to reach the web server. This configuration helps to precisely control which traffic should be blocked, focusing the Deny policy on the intended destination.
Reference:
FortiOS 7.4.1 Administration Guide: Deny matching with a policy with a virtual IP applied FortiOS 7.4.1 Administration Guide: Configuring Policies with VIPs

NO.6 FortiGate is integrated with FortiAnalyzer and FortiManager.
When a firewall policy is created, which attribute is added to the policy to improve functionality and to support recording logs to FortiAnalyzer or FortiManager?

A. Log ID

B. Policy ID

C. Sequence ID

D. Universally Unique Identifier

Answer: D

Explanation:
When a firewall policy is created in FortiGate integrated with FortiAnalyzer and FortiManager, a Universally Unique Identifier (UUID) is added to the policy to support logging and management.

NO.7 An organization requires remote users to send external application data running on their PCs and access FTP resources through an SSUTLS connection.
Which FortiGate configuration can achieve this goal?

A. SSL VPN quick connection

B. SSL VPN tunnel

C. SSL VPN bookmark

D. Zero trust network access

Answer: B

Explanation:

An SSL VPN tunnel allows remote users to securely connect to the organization's network and transmit all traffic, including external application data and FTP resources, through an encrypted SSL/TLS connection. This ensures secure access to the network while supporting various protocols such as FTP and other application-specific traffic from the user's PC.

NO.8 Which statement about the deployment of the Security Fabric in a multi-VDOM environment is true?

A. Downstream devices can connect to the upstream device from any of their VDOMs

B. Each VDOM in the environment can be part of a different Security Fabric

C. VDOMs without ports with connected devices are not displayed in the topology

D. Security rating reports can be run individually for each configured VDOM

Answer: C

Explanation:

"When you configure FortiGate devices in multi-vdom mode and add them to the Security Fabric, each VDOM with its assigned ports is displayed when one or more devices are detected. Only the ports with discovered and connected devices appear in the Security Fabric view and, because of this, you must enable Device Detection on ports you want to have displayed in the Security Fabric. VDOMs without ports with connected devices are not displayed. All VDOMs configured must be part of a single Security Fabric."

NO.9 Which two statements are true regarding FortiGate HA configuration synchronization? (Choose two.)

A. Checksums of devices are compared against each other to ensure configurations are the same.

B. Incremental configuration synchronization can occur only from changes made on the primary FortiGate device.

C. Incremental configuration synchronization can occur from changes made on any FortiGate device within the HA cluster

D. Checksums of devices will be different from each other because some configuration items are not synced to other HA members.

Answer: A,C

Explanation:

"After the initial synchronization is complete, whenever a change is made to the configuration of an HA cluster device (primary or secondary), incremental synchronization sends the same configuration change to all other cluster devices over the HA heartbeat link"