VCE & PDF
GeekCert.com

156-315.81^{Q&As}

Check Point Certified Security Expert R81

Pass CheckPoint 156-315.81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/156-315-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don\'t have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

A. fw ctl multik dynamic_dispatching on

B. fw ctl multik dynamic_dispatching set_mode 9

C. fw ctl multik set_mode 9

D. fw ctl multik pq enable

Correct Answer: C

To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. You can enable them by using the command fw ctl multik set_mode

9. This command sets the SecureXL mode to 9, which means that Priority Queues are enabled and Dynamic Dispatcher is fully enabled. References: SecureXL Mechanism

QUESTION 2

Which command collects diagnostic data for analyzing customer setup remotely?

A. cpinfo

B. migrate export

C. sysinfo

D. cpview

Correct Answer: A

CPInfo is an auto-updatable utility that collects diagnostics data on a customer\'s machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth

analysis of customer\'s configuration and environment settings.

References:

QUESTION 3

If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is

necessary to be completed for it to function properly?

A. Nothing - the proxy ARP is automatically handled in the R81 version

B. Add the proxy ARP configurations in a file called /etc/conf/local.arp

C. Add the proxy ARP configurations in a file called $FWDIR/conf/local.arp

D. Add the proxy ARP configurations in a file called $CPDIR/conf/local.arp

Correct Answer: C

If an administrator wants to add manual NAT for addresses not owned by the Check Point firewall, they also need to add the proxy ARP configurations in a file called $FWDIR/conf/local.arp. This file contains the mappings between the IP addresses and the MAC addresses of the NATed hosts. The proxy ARP feature allows the firewall to answer ARP requests on behalf of the NATed hosts and forward the traffic to them. The local.arp file needs to be edited manually and reloaded with the command arp -f $FWDIR/conf/local.arp. References: R81 Security Management Administration Guide, page 1014.

QUESTION 4

Your manager asked you to check the status of SecureXL, and its enabled templates and features. What command will you use to provide such information to manager?

A. fw accel stat

B. fwaccel stat

C. fw acces stats

D. fwaccel stats

Correct Answer: B

The fwaccel stat command displays the status of SecureXL, and its enabled templates and features. The other commands are either incorrect or incomplete. References: [SecureXL Commands]

QUESTION 5

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

A. assign privileges to users.

B. edit the home directory of the user.

C. add users to your Gaia system.

D. assign user rights to their home directory in the Security Management Server.

Correct Answer: D

The WebUI can be used to manage user accounts and assign privileges to users. It can also add users to your Gaia system and edit the home directory of the user. However, it cannot assign user rights to their home directory in the

Security Management Server1. References: Check Point Resource Library, page 3.