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.passapply.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

QUESTION 1

You need to change the number of firewall Instances used by CoreXL. How can you achieve this goal?

A. edit fwaffinity.conf; reboot required

B. cpconfig; reboot required

C. edit fwaffinity.conf; reboot not required

D. cpconfig; reboot not required

Correct Answer: B

To change the number of firewall instances used by CoreXL, the cpconfig command must be used, followed by a reboot. CoreXL is a technology that improves the performance of the Security Gateway by using multiple cores to handle concurrent connections. The number of firewall instances determines how many cores are dedicated to CoreXL. The cpconfig command allows the administrator to configure various settings on the Security Gateway, including the number of firewall instances. After changing this setting, a reboot is required for the changes to take effect. The other commands are either incorrect or do not require a reboot.

QUESTION 2

What Factor preclude Secure XL Templating?

A. Source Port Ranges/Encrypted Connections

B. IPS

C. ClusterXL in load sharing Mode

D. CoreXL

Correct Answer: A

SecureXL Templating is a feature that accelerates the processing of packets that belong to the same connection or session by creating a template for the first packet and applying it to the subsequent packets. SecureXL Templating is precluded by factors that prevent the creation of a template, such as source port ranges, encrypted connections, NAT, QoS, etc. References: SecureXL Mechanism

QUESTION 3

You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

A. fw unloadlocal

B. fw unloadpolicy

C. fwm unload local

D. fwm unload policy

Correct Answer: A

The command fw unloadlocal removes the current security policy from the local gateway and returns it to its initial state2. This command can be used as a last resort to restore traffic flow through the gateway if the policy is causing problems. The command fw unloadpolicy is not valid, and the commands fwm unload local and fwm unload policy are used to remove policies from remote gateways3. References: 2: Check Point Software, Getting Started, Unloading Security Policies;

3: Check Point Software, Getting Started, Unloading Security Policies from Remote Gateways.

QUESTION 4

What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?

A. test_connectivity_ad

B. test_ldap_connectivity

C. test_ad_connectivity

D. ad_connectivity_test

Correct Answer: C

The CLI utility that runs connectivity tests from a Security Gateway to an AD domain controller is test_ad_connectivity -d . This command tests the connectivity between the gateway and the domain controller using LDAP, Kerberos, and WMI protocols. It also verifies the identity awareness configuration and shows the relevant logs3. The other options are not valid commands for testing AD connectivity. References: 3: Check Point Software, Getting Started, Testing Active Directory Connectivity.

QUESTION 5

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust.

B. The Security Gateway name cannot be changed in command line without re- establishing trust.

C. The Security Management Server name cannot be changed in SmartConsole without re- establishing trust.

D. The Security Management Server IP-address cannot be changed without re-establishing the trust.

Correct Answer: A

After trust has been established between the Check Point components, the Security Gateway IP address cannot be changed without re-establishing the trust. This is because the trust is based on the Secure Internal Communication (SIC) mechanism, which uses certificates to authenticate and encrypt the communication. The certificates are issued by the Internal Certificate Authority (ICA) of the Security Management Server / Domain Management Server, and contain the name and IP address of the component. Therefore, if the IP address of a component is changed, the certificate will become invalid and the trust will be lost. To restore the trust, the certificate must be renewed or reissued by the ICA12.

However, there are some exceptions to this rule. The Security Gateway name can be changed in command line without re-establishing trust, as long as the IP address remains the same. This is because the SIC mechanism does not rely on the hostname, but on the IP address and the SIC name (which is usually derived from the hostname, but can be manually changed). The Security Management Server name can be changed in SmartConsole without re-establishing trust, as long as the IP address remains the same. This is because SmartConsole uses a different mechanism to connect to the Security Management Server, which does not depend on the SIC certificate. The Security Management Server IP address can be changed without re-establishing trust, as long as some steps are followed to update the Check Point Registry file on the managed Security Gateways / Cluster Members / VSX Virtual Devices. This is because the Registry file contains the IP address of the ICA, which is used for certificate renewal. If the Registry file is not updated, then the certificate renewal will fail and the trust will be lost3. References: 1: Check Point R81 Security Administration Guide - Check Point Software, page 162 2: Check Point R81 Security Engineering Guide - Check Point Software, page 162 3: How to renew SIC after changing IP Address of Security Management Server - Check Point Software, Solution ID: sk103356