156-315.81 Q&As

Check Point Certified Security Expert R81

QUESTION 1

Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is ________ .

A. Sent to the Internal Certificate Authority.

B. Sent to the Security Administrator.

C. Stored on the Security Management Server.

D. Stored on the Certificate Revocation List.

Correct Answer: D

Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is stored on the Certificate Revocation List (CRL). The CRL is a list of certificates that have been revoked by the Internal Certificate Authority (ICA) and are no longer valid for Secure Internal Communication (SIC). The CRL is signed by the ICA and issued to all the managed Security Gateways the next time a SIC connection is made12. The CRL helps to prevent unauthorized access to the Security Management Server by revoked Security Gateways. References: 1: How to renew SIC after changing IP Address of Security Management Server - Check Point Software, Solution ID: sk43784 2: Check Point R81 Security Engineering Guide - Check Point Software, page 162

QUESTION 2

Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

A. Application Control

B. Firewall

C. Identity Awareness

D. URL Filtering

Correct Answer: C

The verified answer is C. Identity Awareness. Identity Awareness is the Check Point software blade that provides detailed visibility of users, groups, and machines, while also providing application and access control through the creation of accurate, identity-based policies1. Identity Awareness allows you to easily configure network access and auditing based on three items: network location, the identity of a user and the identity of a machine1. Identity Awareness integrates with multiple identity sources, such as Microsoft Active Directory, Cisco Identity Services Engine, and RADIUS Accounting23. Application Control is the Check Point software blade that enables network administrators to identify and control thousands of applications and widgets, and millions of websites, based on categories, risk, and characteristics. Firewall is the Check Point software blade that provides stateful inspection and enforcement of network traffic, and protects against network and application-level attacks. URL Filtering is the Check Point software blade that enables secure web access by blocking access to malicious and inappropriate websites, and enforcing compliance with corporate policies. References: Identity Awareness - Check Point Software1 Check Point Integrated Security Architecture - Check Point Software2 Cisco Identity Services Engine and Check Point Integration3 Application Control - Check Point Software Firewall - Check Point Software URL Filtering - Check Point Software

QUESTION 3

Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?

A. The CoreXL FW instanxces assignment mechanism is based on Source MAC addresses, Destination MAC addresses

B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores

C. The CoreXL FW instances assignment mechanism is based on IP Protocol type

D. The CoreXl FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP `Protocol\\' type

Correct Answer: B

The statement that is most correct regarding about "CoreXL Dynamic Dispatcher" is: The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores. CoreXL Dynamic Dispatcher is a feature that allows the Security Gateway to dynamically assign connections to the most available CoreXL FW instance, based on the CPU core utilization. This improves the performance and load balancing of the Security Gateway, especially when handling connections with different processing requirements. The other statements are either incorrect or describe the CoreXL Static Dispatcher mechanism, which assigns connections based on a hash function of the Source IP, Destination IP, and IP Protocol type.

QUESTION 4

Native Applications require a thin client under which circumstances?

A. If you want to use a legacy 32-Bit Windows OS

B. If you want to use a VPN Client that is not officially supported by the underlying operating system

C. If you want to have assigned a particular Office Mode IP address.

D. If you are about to use a client (FTP. RDP, ...) that is installed on the endpoint.

Correct Answer: D

Native Applications require a thin client under the circumstance that you are about to use a client (FTP, RDP, etc.) that is installed on the endpoint. A thin client is a lightweight software component that enables secure connectivity for native applications without requiring additional configuration or user intervention. A thin client is automatically downloaded and installed on the endpoint when a user initiates a native application session through Mobile Access Portal or SNX Portal. References: [Check Point Security Expert R81 Mobile Access Administration Guide], page 16.

QUESTION 5

What two ordered layers make up the Access Control Policy Layer?

A. URL Filtering and Network

B. Network and Threat Prevention

C. Application Control and URL Filtering

D. Network and Application Control

Correct Answer: D

What two ordered layers make up the Access Control Policy Layer? Network and Application Control are the two ordered layers that make up the Access Control Policy Layer. The Network layer controls network access based on source, destination, service, time, etc. The Application Control layer controls application access based on users, groups, applications, content categories, etc. The Network layer is always processed before the Application Control layer. References: R81 Security Management Administration Guide, page 29.