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.pass4itsure.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

Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

A. Both License (.lic) and Contract (.xml) files

B. cp.macro

C. Contract file (.xml)

D. license File (.lic)

Correct Answer: B

cp.macro is an electronically signed file used by Check Point to translate the features in the license into a code. It is located in the $FWDIR/conf directory on the Security Management Server. The cp.macro file contains a list of features and their corresponding codes, which are used to generate the license file (.lic) based on the contract file (.xml). The license file (.lic) is then installed on the Security Gateway or Security Management Server to activate the licensed features. References: Check Point R81 Licensing and Contract Administration Guide, page 10

QUESTION 2

What is the mechanism behind Threat Extraction?

A. This a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender.

B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient.

C. This is a new mechanism to identify the IP address of the sender of malicious codes and put it into the SAM database (Suspicious Activity Monitoring).

D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast.

Correct Answer: D

Threat Extraction is a technology that removes potentially malicious features that are known to be risky from files (macros, embedded objects and more), rather than determining their maliciousness. By cleaning the file before it enters the organization, Threat Extraction preemptively prevents both known and unknown threats, providing better protection against zero-day attacks1. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast2. The other options are either incorrect or irrelevant to the mechanism behind Threat Extraction. References: Threat Extraction (CDR) - Check Point Software, Check Point Document Threat Extraction Technology

QUESTION 3

To add a file to the Threat Prevention Whitelist, what two items are needed?

A. File name and Gateway

B. Object Name and MD5 signature

C. MD5 signature and Gateway

D. IP address of Management Server and Gateway

Correct Answer: B

To add a file to the Threat Prevention Whitelist, you need two items:

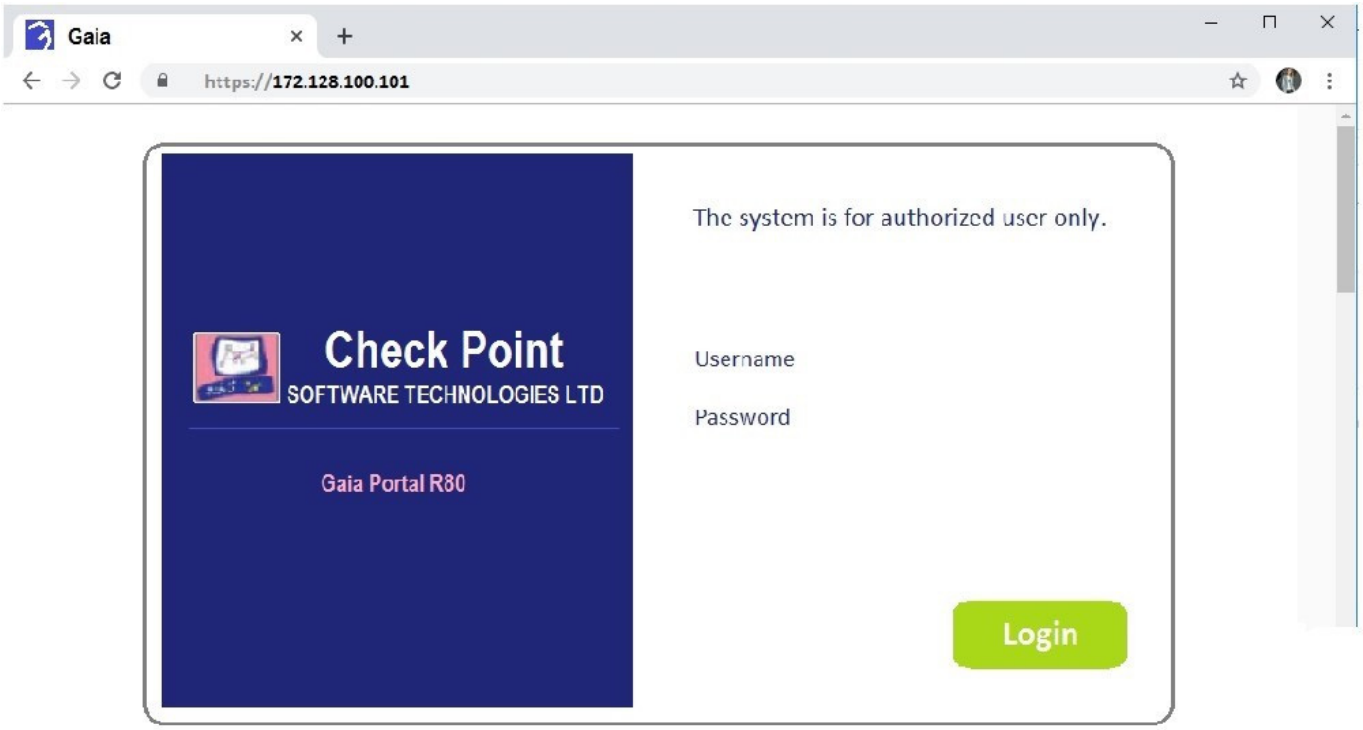
B. Object Name and MD5 signature

You need the Object Name to identify the file or object you want to whitelist, and the MD5 signature to specify the unique hash value of that file. The MD5 signature ensures that the specific file you want to whitelist is identified accurately.

References: Check Point Certified Security Expert R81 Study Guide, Threat Prevention Administration Guide.

QUESTION 4

Kofi, the administrator of the ALPHA Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



A. set web ssl-port

B. set Gaia-portal port

C. set Gaia-portal https-port

D. set web https-port

Correct Answer: A

The CLISH command to change the default Gaia WebUI Portal port number is set web ssl-port . This command will change the port that the WebUI listens on for HTTPS connections. After changing the port, you need to save the configuration with save config and verify that the change was applied with show web ssl- port. You also need to update the Main URL in the Platform Portal section of the gateway object in SmartConsole and install the policy.

QUESTION 5

Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?

A. Windows Management Instrumentation (WMI)

B. Hypertext Transfer Protocol Secure (HTTPS)

C. Lightweight Directory Access Protocol (LDAP)

D. Remote Desktop Protocol (RDP)

Correct Answer: A

Windows Management Instrumentation (WMI) is a protocol that allows remote management and monitoring of Windows systems. It is used by AD Query to connect to the Active Directory Domain Controllers and query them for user and computer information. AD Query uses WMI to get real-time updates on user logon events, group membership changes, and computer status changes. WMI is not the same as LDAP, which is a protocol for accessing and modifying directory services. HTTPS and RDP are also different protocols that are not used by AD Query. References: Check Point R81 Identity Awareness Administration Guide, page 17