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

For Management High Availability, which of the following is NOT a valid synchronization status?

A. Collision

B. Down

C. Lagging

D. Never been synchronized

Correct Answer: B

For Management High Availability, the valid synchronization status options are:

A. Collision

B. Down

C. Lagging

D. Never been synchronized

In this context, "Down" indicates that the synchronization is not functioning correctly or that the standby management server is not reachable. This is a valid synchronization status, so the answer is not B.

References: Check Point Certified Security Expert (CCSE) R81 documentation and learning resources.

QUESTION 2

Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

A. cpwd

B. fwd

C. cpd

D. fwm

Correct Answer: D

Firewall Management (fwm) is available on any management product, including Multi- Domain and on products that requite direct GUI access, such as SmartEvent, It provides the following: ?GUI Client communication ?Database manipulation ?Policy Compilation ?Management HA sync

QUESTION 3

What are the modes of SandBlast Threat Emulation deployment?

A. Cloud, Smart-1 and Hybrid

B. Cloud. OpenServer and Vmware

C. Cloud, Appliance and Private

D. Cloud, Appliance and Hybrid

Correct Answer: D

SandBlast Threat Emulation is a technology that protects against zero-day and unknown malware by inspecting files in a secure sandbox environment and emulating their behavior. SandBlast Threat Emulation can be deployed in three modes: Cloud, Appliance and Hybrid1. Cloud mode: The files are sent to the Check Point cloud service for emulation. This mode does not require any additional hardware or software installation. It is the easiest and most cost-effective way to deploy SandBlast Threat Emulation. Appliance mode: The files are sent to a dedicated appliance (TE1000X, TE2500X, or TE100X) for emulation. This mode provides the highest level of performance and scalability, as well as data privacy and compliance. It is suitable for large organizations with high security and throughput requirements. Hybrid mode: The files are first sent to the Check Point cloud service for emulation, and if the cloud service cannot determine the verdict, they are then sent to a dedicated appliance for further analysis. This mode combines the benefits of both cloud and appliance modes, offering fast response time and high accuracy. References: 1: SandBlast Threat Emulation Deployment Modes

QUESTION 4

You want to gather and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

A. SmartEvent Client Info

B. SecuRemote

C. Check Point Protect

D. Check Point Capsule Cloud

Correct Answer: C

Check Point Protect is a lightweight app that can be used to gather and analyze threats to your mobile device. It provides real-time threat intelligence, device posture assessment, and secure browsing protection3. The other applications are either not designed for mobile devices, or do not offer threat analysis features. References: R81 CCSA and CCSE exams released featuring Promo for... - Check Point ..., Check Point Protect - Apps on Google Play

QUESTION 5

In what way are SSL VPN and IPSec VPN different?

A. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless

B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not

C. IPSec VPN does not support two factor authentication, SSL VPN does support this

D. IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only.

Correct Answer: D

The way SSL VPN and IPSec VPN are different is that IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only. SSL VPN and IPSec VPN are two types of VPN technologies that provide secure remote access to network resources over the internet. SSL VPN uses SSL/TLS protocol to establish an encrypted tunnel between the client and the server, and does not require any additional software or hardware on the client side. IPSec VPN uses IPSec protocol to establish an encrypted tunnel between the client and the server, and requires a dedicated virtual adapter on the client side to handle the IPSec traffic. The other options are either incorrect or not relevant to SSL VPN and IPSec VPN.