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

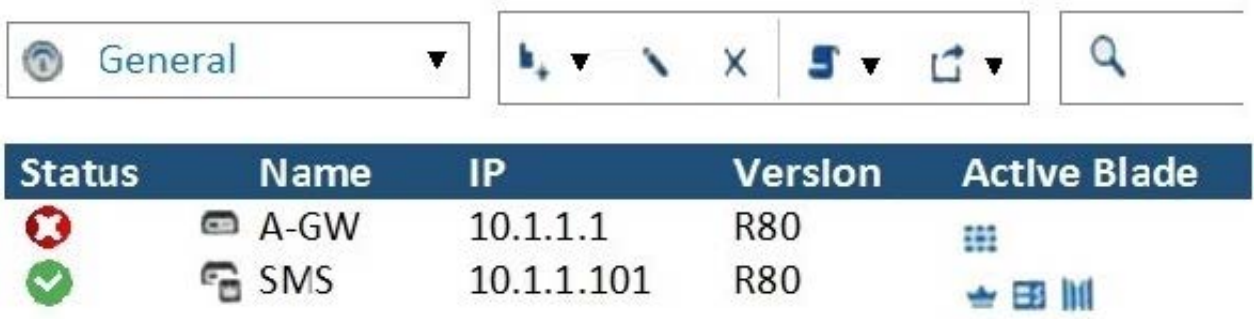
100% Passing Guarantee
100% Money Back Assurance

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

What does it mean if Deyra sees the gateway status? (Choose the BEST answer.)



A. SmartCenter Server cannot reach this Security Gateway.

B. There is a blade reporting a problem.

C. VPN software blade is reporting a malfunction.

D. Security Gateway\\'s MGNT NIC card is disconnected.

Correct Answer: B

If Deyra sees the gateway status as shown in the image, it means that there is a blade reporting a problem. The red exclamation mark indicates that one or more blades on the gateway have an issue that needs attention. The issue could be related to configuration, license, policy, or other factors. Deyra can hover over the icon to see more details about the problem. References: Training and Certification | Check Point Software, New Courses and Certificates for R81.20 - Check Point CheckMates

QUESTION 2

Which Operating Systems are supported for the Endpoint Security VPN?

A. Windows and x86 Solaris

B. Windows and macOS computers

C. Windows and SPARC Solaris

D. Windows and Red Hat Linux

Correct Answer: B

Endpoint Security VPN is a lightweight remote access client that supports Windows and macOS computers. It provides secure connectivity to corporate resources using L2TP/IPSec, SSL, or Check Point\\'s proprietary VPN protocol. Endpoint Security VPN also integrates with other Endpoint Security products such as SandBlast Agent, Full Disk Encryption, Media Encryption, and Firewall. References: Check Point R81 Endpoint Security VPN Administration Guide, page 5

QUESTION 3

Which is not a blade option when configuring SmartEvent?

A. Correlation Unit

B. SmartEvent Unit

C. SmartEvent Server

D. Log Server

Correct Answer: B

SmartEvent Unit is not a blade option when configuring SmartEvent. SmartEvent is a unified security event management solution that provides visibility, analysis, and reporting of security events across multiple Check Point products. SmartEvent consists of three main components: SmartEvent Server, Correlation Unit, and Log Server. SmartEvent Server is responsible for storing and displaying security events in SmartConsole and SmartEventWeb. Correlation Unit is responsible for collecting and correlating logs from various sources and generating security events based on predefined or custom scenarios. Log Server is responsible for receiving and indexing logs from Security Gateways and other Check Point modules. SmartEvent Unit is not a valid component or blade of SmartEvent.

QUESTION 4

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 5

What is required for a site-to-site VPN tunnel that does not use certificates?

A. Pre-Shared Secret

B. RSA Token

C. Unique Passwords

D. SecureID

Correct Answer: A

A pre-shared secret is a secret key that is shared between the two VPN peers before establishing a secure connection. It is used to authenticate the VPN peers and encrypt the VPN traffic. A pre-shared secret is required for a site-to-site VPN tunnel that does not use certificates, because certificates are another way of authenticating the VPN peers using public key cryptography. Without certificates, the VPN peers need to have a common secret key that only they know. References: Check Point R81 VPN Administration Guide, page 13