VCE & PDF
GeekCert.com

156-215.81^{Q&As}

Check Point Certified Security Administrator R81

Pass CheckPoint 156-215.81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/156-215-81.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 are valid authentication methods for mutual authenticating the VPN gateways?

A. Pre-shared Secret and PKI Certificates

B. PKI Certificates and Kerberos Tickets

C. Pre-Shared Secrets and Kerberos Ticket

D. PKI Certificates and DynamiciD OTP

Correct Answer: A

This answer is correct because these are two valid methods for mutually authenticating the VPN gateways, which means that both sides of the communication verify each other\\'s identity using a shared secret or a public key certificate. A preshared secret is a password or a passphrase that both gateways know and use to encrypt and decrypt the VPN traffic. A PKI certificate is a digital document that contains the public key and other information that helps identify the gateway, such as the issuer, the subject, and the expiration date. The certificate is signed by a trusted certificate authority (CA) that vouches for the authenticity of the gateway. The other answers are not correct because they either include invalid or irrelevant methods for mutual authentication. PKI certificates and Kerberos tickets are not compatible methods for mutual authentication, because Kerberos tickets are issued by a Kerberos server and not by a CA. Pre-shared secrets and Kerberos tickets are also not compatible methods for mutual authentication, because they use different protocols and encryption algorithms. PKI certificates and DynamiciD OTP are not valid methods for mutual authentication, because DynamiciD OTP is a one-time password that is used for user authentication, not for gateway authentication.

What is mutual authentication? | Two-way authentication Mutual authentication - AWS Client VPN VPN authentication options - Windows Security Mutual Authentication | Top 3 Methods of Mutual Authentication Authentication methods and features - Microsoft Entra

QUESTION 2

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does what with the data?

A. Cache the data to speed up its own function.

B. Share the data to the ThreatCloud for use by other Threat Prevention blades.

C. Log the traffic for Administrator viewing.

D. Delete the data to ensure an analysis of the data is done each time.

Correct Answer: B

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does share the data to the ThreatCloud for use by other Threat Prevention blades. The ThreatCloud is a collaborative network and cloud- driven knowledge base that delivers real-time dynamic security intelligence to security gateways. The Threat Prevention gateway can send and receive updates from the ThreatCloud about new threats and malicious data signatures. References: [Check Point R81 Threat Prevention Administration Guide]

QUESTION 3

What is the default shell for the command line interface?

A. Clish

B. Admin

C. Normal

D. Expert

Correct Answer: A

Clish is the default shell for the command line interface. It is a user-friendly shell that provides a menu-based and a command-line mode. Admin, Normal, and Expert are not valid shell names.

QUESTION 4

When changes are made to a Rule base, it is important to _____ to enforce changes.

A. Publish database

B. Activate policy

C. Install policy

D. Save changes

Correct Answer: A

When changes are made to a Rule base, it is important to Publish database to enforce changes. Publishing database saves the changes to the database and makes them available to other administrators. Installing policy applies the changes to the Security Gateways. References: Check Point R81 Security Management Administration Guide, [Check Point R81 SmartConsole R81 Resolved Issues], [Check Point R81 Firewall Administration Guide]

QUESTION 5

Fill in the blank RADIUS protocol uses_____to communicate with the gateway

A. UDP

B. CCP

C. TDP

D. HTTP

Correct Answer: A

RADIUS protocol uses UDP (User Datagram Protocol) to communicate with the gateway. UDP is a connectionless protocol that does not require a handshake or acknowledgment before sending or receiving data2. References: [Check Point R81 Identity Awareness Administration Guide], page 14.