ACTUAL
TEST DUMPS

Free Questions for 156-215.81 by actualtestdumps

Shared by Williamson on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is required for a certificate-based VPN tunnel between two gateways with separate management systems?

Options:

A- Shared Secret Passwords

B- Unique Passwords

C- Shared User Certificates

D- Mutually Trusted Certificate Authorities

Answer:

D

Explanation:

This answer is correct because for a certificate-based VPN tunnel, both gateways need to have a certificate issued by a certificate authority (CA) that they trust1.A CA is a trusted entity that verifies the identity of the gateways and signs their certificates2.The gateways can either use the same CA or different CAs, as long as they trust each other's CA3. This way, the gateways can authenticate each other using their certificates and establish a secure VPN tunnel.

The other answers are not correct because they are either irrelevant or incompatible with certificate-based VPN tunnel.Shared secret passwords and unique passwords are used for pre-shared key (PSK) authentication, which is a different method than certificate authentication4. PSK authentication is less secure and more vulnerable to brute force attacks than certificate authentication. Shared user certificates are not used for gateway authentication, but for user authentication, which is a different level of authentication than gateway authentication. User authentication is optional and can be used in addition to gateway authentication to provide more granular access control.

Configure server settings for P2S VPN Gateway connections - certificate authentication

VPN certificates and how they work

Create Certificate Based Site to Site VPN between 2 Check Point Gateways

HowTo Set Up Certificate Based VPNs with Check Point Appliances

Question 2

Question Type: **MultipleChoice**

Which encryption algorithm is the least secured?

Options:

A- 3DES

B- AES-128

C- DES

D- AES-256

Answer:

C

Explanation:

This answer is correct because DES (Data Encryption Standard) is the least secured encryption algorithm among the options given.DES uses a 56-bit key, which is too short and can be easily cracked by brute force attacks1.DES also suffers from other weaknesses, such as weak keys, complementation property, and linear cryptanalysis2.

The other answers are not correct because they are more secured encryption algorithms than DES.3DES (Triple DES) is an improvement over DES that applies DES three times with different keys, resulting in a 168-bit key3. AES-128 and AES-256 are variants of AES (Advanced Encryption Standard) that use 128-bit and 256-bit keys respectively. AES is considered to be the most secure symmetric encryption algorithm and is widely used for data protection.

What is DES encryption, and why was it replaced?

Data Encryption Standard - Wikipedia

What is 3DES encryption?

[What is AES encryption and how does it work?]

Question 3

Question Type: **MultipleChoice**

Which of the following is a valid deployment option?

Options:

A- CloudSec deployment

B- Disliked deployment

C- Router only deployment

D- Standalone deployment

Answer:

D

Explanation:

This answer is correct because a standalone deployment is a valid option for installing a Check Point Security Gateway and a Security Management Server on the same machine1.This option is suitable for small or medium-sized networks that do not require high availability or load balancing1.

The other answers are not correct because they are either invalid or irrelevant options for deployment.CloudSec deployment is not a valid option, but it might be confused with CloudGuard, which is a Check Point solution for securing cloud environments2.Disliked deployment is not a valid option, but it might be a typo for Distributed deployment, which is a valid option for installing a Check Point Security Gateway and a Security Management Server on separate machines1.Router only deployment is not a valid option, but it might be confused with Router mode, which is a configuration option for a Check Point Security Gateway that enables it to act as a router and forward packets between interfaces3.

Gaia R81.20 Administration Guide

CloudGuard Network Security

Configuring Router Mode in Gaia Clish

Question 4

Question Type: MultipleChoice

What are valid authentication methods for mutual authenticating the VPN gateways?

Options:

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

Answer:

A

Explanation:

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 certificate1.A pre-shared secret is a password or a passphrase that both gateways know and use to encrypt and decrypt the VPN traffic2.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 date3.The certificate is signed by a trusted certificate authority (CA) that vouches for the authenticity of the gateway3.

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 CA4.Pre-shared secrets and Kerberos tickets are also not compatible methods for mutual authentication, because they use different protocols and encryption algorithms4.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 authentication5.

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 5

Question Type: MultipleChoice

Which command shows detailed information about VPN tunnels?

Options:

A- cat $FWDIR/conf/vpn.conf

B- vpn tu tlist

C- vpn tu

D- cpview

Answer:

C

Explanation:

This answer is correct because thevpn tucommand is used for VPN tunnel management and shows detailed information about VPN tunnels, such as the tunnel ID, peer IP, encryption domain, and status1.This command will bring up a menu for you to choose from, such as list all IPsec SAs, delete all IPsec SAs, or delete IPsec SA for given peer1.

The other answers are not correct because they either show different information or do not exist as commands.Thecat $FWDIR/conf/vpn.confcommand shows the VPN configuration file, which contains the VPN domains, communities, and encryption settings2.Thevpn tu tlistcommand does not exist, but it might be confused with thevpn tunnelutil tlistcommand, which shows the tunnel utilization statistics3.Thecpviewcommand shows the Check Point real-time performance monitoring tool, which displays various system and network parameters, such as CPU, memory, disk, interfaces, and VPN4.

How to use the "vpn tu" command for VPN tunnel management

New VPN daemons in R81.10 / R81.20 - Check Point CheckMates

Remote Access VPN R81.20 Administration Guide - Check Point Software

Remote Access VPN R81 Administration Guide - Check Point Software

Question 6

Question Type: **MultipleChoice**

What are the software components used by Autonomous Threat Prevention Profiles in R8I.20 and higher?

Options:

A- Sandbox, ThreatCloud, Zero Phishing, Sanitization, C&C Protection, JPS, File and URL Reputation

B- IPS, Threat Emulation and Threat Extraction

C- Sandbox, ThreatCloud, Sanitization, C&C Protection, IPS

D- IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction

Answer:

D

Explanation:

This answer is correct because these are the software components that are used by the pre-defined Autonomous Threat Prevention Profiles in R81.20 and higher1.These profiles provide zero-maintenance protection from zero-day threats and continuously and autonomously ensure that your protection is up-to-date with the latest cyber threats and prevention technologies2.

The other answers are not correct because they either include software components that are not part of the Autonomous Threat Prevention Profiles, such as Sandbox, ThreatCloud, Zero Phishing, Sanitization, C&C Protection, JPS, File and URL Reputation, or they omit some of the software components that are part of the Autonomous Threat Prevention Profiles, such as Anti-Bot, Anti-Virus, and Macro Extraction.

Autonomous Threat Prevention Management - Check Point Software

Check Point Quantum R81.20 (Titan) Release

Threat Prevention R81.20 Best Practices - Check Point Software

Check Point R81

Question 7

Question Type: MultipleChoice

Aggressive Mode in IKEv1 uses how many packages for negotiation?

Options:

A- 6

B- 3

C- depends on the make of the peer gateway

D- 5

Answer:

B

Explanation:

Aggressive Mode in IKEv1 usesthree packetsfor negotiation, with all data required for the SA passed by the initiator1. The responder sends the proposal, key material, and ID, and authenticates the session in the next packet.The initiator replies and authenticates the session1.

The other answers are not correct because they either refer to the Main Mode in IKEv1, which uses six packets for negotiation2, or they are irrelevant to the number of packets used in Aggressive Mode.

Understand IPsec IKEv1 Protocol - Cisco

Negotiation modes for phase 1 - IBM

FAQ-What are the differences between IKEv1 and IKEv2- Huawei

Question 8

Question Type: MultipleChoice

You had setup the VPN Community NPN-Stores' with 3 gateways. There are some issues with one remote gateway(l .1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways.

Options:

A- action:''Key Install' AND 1.1.1.1 AND Quick Mode

B- Blade:''VPN''AND VPN-Stores AND Main Mode

C- action:"Key Install" AND 1.1.1.1 AND Main Mode

D- Blade:"VPN"AND VPN-Stores AND Quick Mode

Answer:

A

Explanation:

This log filter will show only the logs that have the action of "Key Install", which means that the Security Gateway installed a new encryption key for the VPN tunnel1. It will also show only the logs that have the IP address of 1.1.1.1, which is the remote gateway that has some issues.Finally, it will show only the logs that have the Quick Mode, which is the IKE Phase 2 negotiation that establishes the agreed networks for both gateways2.

The other log filters are not correct because they either include the Main Mode, which is the IKE Phase 1 negotiation that establishes the secure channel between the gateways2, or they do not specify the IP address of the remote gateway.

Logging and Monitoring R81.20 Administration Guide

Remote Access VPN R81.20 Administration Guide

Remote Access VPN R81 Administration Guide

Question 9

Question Type: **MultipleChoice**

Which of the following statements about Site-to-Site VPN Domain-based is NOT true?

Options:

A- Route-based--- The Security Gateways will have a Virtual Tunnel Interface (VTI) for each VPN Tunnel with a peer VPN Gateway. The Routing Table can have routes to forward traffic to these VTIs. Any traffic routed through a VTI is automatically identified as VPN Traffic and is passed through the VPN Tunnel associated with the VTI.

B- Domain-based--- VPN domains are pre-defined for all VPN Gateways.
A VPN domain is a service or user that can send or receive VPN traffic through a VPN Gateway.

C- Domain-based--- VPN domains are pre-defined for all VPN Gateways. A VPN domain is a host or network that can send or receive VPN traffic through a VPN Gateway.

D- Domain-based--- VPN domains are pre-defined for all VPN Gateways.
When the Security Gateway encounters traffic originating from one VPN Domain with the destination to a VPN Domain of another VPN Gateway, that traffic is identified as VPN traffic and is sent through the VPN Tunnel between the two Gateways.

Answer:

B

Explanation:

Domain-based--- VPN domains are pre-defined for all VPN Gateways. A VPN domain is a service or user that can send or receive VPN traffic through a VPN Gateway.

This statement isnot truebecause a VPN domain isnota service or user, but ahost or networkthat can send or receive VPN traffic through a VPN Gateway1.This is the definition given in the Site to Site VPN R81 Administration Guide1.The other statements are true according to the same guide1.

Remote Access VPN R81.20 Administration Guide

Site to Site VPN R81 Administration Guide

DeepDive Webinar - R81.20 Seamless VPN Connection to Public Cloud

Question 10

Question Type: **MultipleChoice**

What is the order of NAT priorities?

Options:

A- IP pool NAT static NAT. hide NAT

B- Static NAT hide NAT, IP pool NAT

C- Static NAT, IP pool NAT hide NAT

D- Static NAT automatic NAT hide NAT

Answer:

C

Explanation:

The order of NAT priorities is Static NAT, IP pool NAT, and hide NAT. Static NAT has the highest priority because it is a one-to-one mapping of a private IP address to a public IP address. IP pool NAT has the second highest priority because it is a one-to-many mapping of a private IP address to a pool of public IP addresses.Hide NAT has the lowest priority because it is a many-to-one mapping of multiple private IP addresses to a single public IP address1.

Question 11

Question Type: MultipleChoice

Which command is used to add users to or from existing roles?

Options:

A- add rba user <User Name> roles <List>

B- add user <User Name>

C- add rba user <User Name>

D- add user <User Name> roles <List>

Answer:

A

Explanation:

The commandadd rba user <User Name> roles <List>is used to add users to or from existing roles.RBA stands for Role-Based Administration, which is a feature that allows administrators to assign different permissions and access levels to users based on their roles2.