

Exam Questions 156-215.80

Check Point Certified Security Administrator

<https://www.2passeasy.com/dumps/156-215.80/>



NEW QUESTION 1

- (Exam Topic 1)

Which of the following commands can be used to remove site-to-site IPSEC Security Associations (SA)?

- A. vpn tu
- B. vpn ipsec remove -l
- C. vpn debug ipsec
- D. fw ipsec tu

Answer: A

Explanation:

vpn tu

Description Launch the TunnelUtil tool which is used to control VPN tunnels.

Usage vpn tu vpn tunnelutil Example vpn tu Output

NEW QUESTION 2

- (Exam Topic 1)

Which of the following is NOT a component of a Distinguished Name?

- A. Organization Unit
- B. Country
- C. Common name
- D. User container

Answer: D

Explanation:

Distinguished Name Components

CN=common name, OU=organizational unit, O=organization, L=locality, ST=state or province, C=country name

NEW QUESTION 3

- (Exam Topic 1)

Which of the following are types of VPN communicates?

- A. Pentagon, star, and combination
- B. Star, octagon, and combination
- C. Combined and star
- D. Meshed, star, and combination

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

What does the “unknown” SIC status shown on SmartConsole mean?

- A. The SMS can contact the Security Gateway but cannot establish Secure Internal Communication.
- B. SIC activation key requires a reset.
- C. The SIC activation key is not known by any administrator.
- D. There is no connection between the Security Gateway and SMS.

Answer: D

Explanation:

The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is Unknown then there is no connection between the Gateway and the Security Management server. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

NEW QUESTION 5

- (Exam Topic 1)

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protect BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

- A. IPS and Application Control
- B. IPS, anti-virus and anti-bot
- C. IPS, anti-virus and e-mail security
- D. SandBlast

Answer: D

Explanation:

SandBlast Zero-Day Protection

Hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. Zero-day exploit protection from Check Point provides a deeper level of inspection so you can prevent more malware and zero-day attacks, while ensuring quick delivery of safe content to your users.

NEW QUESTION 6

- (Exam Topic 1)

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Stateful Inspection
- C. Packet Filtering
- D. Application Layer Firewall

Answer: B

NEW QUESTION 7

- (Exam Topic 1)

What are the three essential components of the Check Point Security Management Architecture?

- A. SmartConsole, Security Management Server, Security Gateway
- B. SmartConsole, SmartUpdate, Security Gateway
- C. Security Management Server, Security Gateway, Command Line Interface
- D. WebUI, SmartConsole, Security Gateway

Answer: A

Explanation:

Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.

Distributed deployment - Security Gateway and the Security Management server are installed on different machines.

Deployments

Basic deployments:

Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.

You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.

The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.

There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.

NEW QUESTION 8

- (Exam Topic 1)

Which of the following statements is TRUE about R80 management plug-ins?

- A. The plug-in is a package installed on the Security Gateway.
- B. Installing a management plug-in requires a Snapshot, just like any upgrade process.
- C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
- D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SmartConsole
- C. SecureClient

D. SmartEvent

Answer: D

Explanation:

There are different deployment scenarios for Check Point software products.

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

NEW QUESTION 10

- (Exam Topic 1)

While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

- A. Security Gateways is not part of the Domain
- B. SmartConsole machine is not part of the domain
- C. SMS is not part of the domain
- D. Identity Awareness is not enabled on Global properties

Answer: B

Explanation:

To enable Identity Awareness:

Log in to SmartDashboard.

From the Network Objects tree, expand the Check Point branch.

Double-click the Security Gateway on which to enable Identity Awareness.

In the Software Blades section, select Identity Awareness on the Network Security tab. The Identity Awareness Configuration wizard opens.

Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers.

Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).

See Choosing Identity Sources.

Note - When you enable Browser-Based Authentication on a Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.

Click Next.

The Integration With Active Directory window opens.

When SmartDashboard is part of the domain, SmartDashboard suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with all of the domain controllers in the organization's Active Directory.

NEW QUESTION 10

- (Exam Topic 1)

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

- A. UserCheck
- B. Active Directory Query
- C. Account Unit Query
- D. User Directory Query

Answer: B

Explanation:

AD Query extracts user and computer identity information from the Active Directory Security Event Logs. The system generates a Security Event log entry when a user or computer accesses a network resource. For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.

Reference : https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

NEW QUESTION 14

- (Exam Topic 1)

The Gaia operating system supports which routing protocols?

- A. BGP, OSPF, RIP
- B. BGP, OSPF, EIGRP, PIM, IGMP
- C. BGP, OSPF, RIP, PIM, IGMP
- D. BGP, OSPF, RIP, EIGRP

Answer: A

Explanation:

The Advanced Routing Suite

The Advanced Routing Suite CLI is available as part of the Advanced Networking Software Blade.

For organizations looking to implement scalable, fault-tolerant, secure networks, the Advanced Networking blade enables them to run industry-standard dynamic routing protocols including BGP, OSPF, RIPv1, and RIPv2 on security gateways. OSPF, RIPv1, and RIPv2 enable dynamic routing over a single autonomous system—like a single department, company, or service provider—to avoid network failures. BGP provides dynamic routing support across more complex networks involving multiple autonomous systems—such as when a company uses two service providers or divides a network into multiple areas with different administrators responsible for the performance of each.

NEW QUESTION 17

- (Exam Topic 1)

What does ExternalZone represent in the presented rule?

- A. The Internet.
- B. Interfaces that administrator has defined to be part of External Security Zone.
- C. External interfaces on all security gateways.
- D. External interfaces of specific gateways.

Answer: B

Explanation:

Configuring Interfaces

Configure the Security Gateway 80 interfaces in the Interfaces tab in the Security Gateway window. To configure the interfaces:

From the Devices window, double-click the Security Gateway 80.

The Security Gateway

window opens.

Select the Interfaces tab.

Select Use the following settings. The interface settings open.

Select the interface and click Edit.

The Edit window opens.

From the IP Assignment section, configure the IP address of the interface:

Select Static IP.

Enter the IP address and subnet mask for the interface.

In Security Zone, select Wireless, DMS, External, or Internal. Security zone is a type of zone, created by a bridge to easily create segments, while maintaining IP addresses and router configurations. Security zones let you choose if to enable or not the firewall between segments.

References:

NEW QUESTION 19

- (Exam Topic 1)

Which of the following is TRUE regarding Gaia command line?

- A. Configuration changes should be done in mgmt_cli and use CLISH for monitoring, Expert mode is used only for OS level tasks.
- B. Configuration changes should be done in expert-mode and CLISH is used for monitoring.
- C. Configuration changes should be done in mgmt-cli and use expert-mode for OS-level tasks.
- D. All configuration changes should be made in CLISH and expert-mode should be used for OS-level tasks.

Answer: D

NEW QUESTION 22

- (Exam Topic 1)

Two administrators Dave and Jon both manage R80 Management as administrators for ABC Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it his in his SmartConsole view?

- A. Jon is currently editing rule no.6 but has Published part of his changes.
- B. Dave is currently editing rule no.6 and has marked this rule for deletion.
- C. Dave is currently editing rule no.6 and has deleted it from his Rule Base.
- D. Jon is currently editing rule no.6 but has not yet Published his changes.

Answer: D

Explanation:

When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited. To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

NEW QUESTION 24

- (Exam Topic 1)

Fill in the blank: The R80 utility fw monitor is used to troubleshoot _____

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues
- D. Phase two key negotiation

Answer: C

Explanation:

Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark

NEW QUESTION 26

- (Exam Topic 1)

Fill in the blank: To build an effective Security Policy, use a _____ and _____ rule.

- A. Cleanup; stealth
- B. Stealth; implicit
- C. Cleanup; default
- D. Implicit; explicit

Answer: A

NEW QUESTION 28

- (Exam Topic 1)

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

- A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
- B. Create a separate Security Policy package for each remote Security Gateway.
- C. Create network object that restrict all applicable rules to only certain networks.
- D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

Answer: B

NEW QUESTION 33

- (Exam Topic 1)

ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house R80 Management to the other administrators in ABC Corp.

How will you describe the new "Publish" button in R80 Management Console?

- A. The Publish button takes any changes an administrator has made in their management session, publishes a copy to the Check Point of R80, and then saves it to the R80 database.
- B. The Publish button takes any changes an administrator has made in their management session and publishes a copy to the Check Point Cloud of R80 and but does not save it to the R80
- C. The Publish button makes any changes an administrator has made in their management session visible to all other administrator sessions and saves it to the Database.
- D. The Publish button makes any changes an administrator has made in their management session visible to the new Unified Policy session and saves it to the Database.

Answer: C

Explanation:

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

NEW QUESTION 37

- (Exam Topic 1)

Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

- A. Security questions
- B. Check Point password
- C. SecurID
- D. RADIUS

Answer: A

Explanation:

Authentication Schemes :- Check Point Password

- Operating System Password
- RADIUS
- SecurID
- TACAS
- Undefined If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

NEW QUESTION 39

- (Exam Topic 1)

Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using ____ .

- A. User Directory
- B. Captive Portal and Transparent Kerberos Authentication
- C. Captive Portal
- D. UserCheck

Answer: B

Explanation:

To enable Identity Awareness:

Log in to SmartDashboard.

From the Network Objects tree, expand the Check Point branch.

Double-click the Security Gateway on which to enable Identity Awareness.

In the Software Blades section, select Identity Awareness on the Network Security tab.

The Identity Awareness

Configuration wizard opens.

Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers

Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

NEW QUESTION 42

- (Exam Topic 1)

What is the purpose of Captive Portal?

- A. It provides remote access to SmartConsole
- B. It manages user permission in SmartConsole
- C. It authenticates users, allowing them access to the Internet and corporate resources
- D. It authenticates users, allowing them access to the Gaia OS

Answer: C

Explanation:

Captive Portal – a simple method that authenticates users through a web interface before granting them access to Intranet resources. When users try to access a protected resource, they get a web page that must be filled out to continue.

Reference : <https://www.checkpoint.com/products/identity-awareness-software-blade/>

NEW QUESTION 47

- (Exam Topic 1)

View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.

- A. The current administrator has read-only permissions to Threat Prevention Policy.
- B. Another user has locked the rule for editing.
- C. Configuration lock is present
- D. Click the lock symbol to gain read-write access.
- E. The current administrator is logged in as read-only because someone else is editing the policy.

Answer: B

Explanation:

Administrator Collaboration

More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

NEW QUESTION 50

- (Exam Topic 1)

Joey wants to configure NTP on R80 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

- A. https://<Device_IP_Address>
- B. https://<Device_IP_Address>:443
- C. https://<Device_IP_Address>:10000
- D. https://<Device_IP_Address>:4434

Answer: A

Explanation:

Access to Web UI Gaia administration interface, initiate a connection from a browser to the default administration IP address: Logging in to the WebUI

Logging in

To log in to the WebUI:

Enter this URL in your browser: <https://<Gaia IP address>>

Enter your user name and password. References:

NEW QUESTION 55

- (Exam Topic 1)

Which type of the Check Point license ties the package license to the IP address of the Security Management Server?

- A. Local
- B. Central
- C. Corporate
- D. Formal

Answer: B

NEW QUESTION 60

- (Exam Topic 1)

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

- A. remove database lock
- B. The database feature has one command lock database override.
- C. override database lock
- D. The database feature has two commands: lock database override and unlock databas
- E. Both will work.

Answer: D

Explanation:

Use the database feature to obtain the configuration lock. The database feature has two commands:

lock database [override].

unlock database

The commands do the same thing: obtain the configuration lock from another administrator.

NEW QUESTION 64

- (Exam Topic 1)

Choose what BEST describes the Policy Layer Traffic Inspection.

- A. If a packet does not match any of the inline layers, the matching continues to the next Layer.
- B. If a packet matches an inline layer, it will continue matching the next layer.
- C. If a packet does not match any of the inline layers, the packet will be matched against the Implicit Clean-up Rule.
- D. If a packet does not match a Network Policy Layer, the matching continues to its inline layer.

Answer: B

NEW QUESTION 66

- (Exam Topic 1)

Which application should you use to install a contract file?

- A. SmartView Monitor
- B. WebUI
- C. SmartUpdate
- D. SmartProvisioning

Answer: C

Explanation:

Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 /

Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.

Open SmartUpdate and from the Launch Menu select 'Licenses & Contracts' -> 'Update Contracts' -> 'From File...' and provide the path to the file you have downloaded in Step #3:

Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.

NEW QUESTION 71

- (Exam Topic 1)

What are the three authentication methods for SIC?

- A. Passwords, Users, and standards-based SSL for the creation of security channels
- B. Certificates, standards-based SSL for the creation of secure channels, and 3DES or AES128 for encryption

- C. Packet Filtering, certificates, and 3DES or AES128 for encryption
- D. Certificates, Passwords, and Tokens

Answer: B

Explanation:

Secure Internal Communication (SIC)

Secure Internal Communication (SIC) lets Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components. SIC is required to install policies on gateways and to send logs between gateways and management servers.

These security measures make sure of the safety of SIC:

Certificates for authentication

Standards-based SSL for the creation of the secure channel

3DES for encryption

References:

NEW QUESTION 73

- (Exam Topic 1)

Fill in the blank: Gaia can be configured using the _____ or _____.

- A. Gaia; command line interface
- B. WebUI; Gaia Interface
- C. Command line interface; WebUI
- D. Gaia Interface; GaiaUI

Answer: C

Explanation:

Configuring Gaia for the First Time In This Section:

Running the First Time Configuration Wizard in WebUI Running the First Time Configuration Wizard in CLI

After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

NEW QUESTION 78

- (Exam Topic 1)

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret is shared and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

Answer: C

NEW QUESTION 80

- (Exam Topic 1)

Which of the following is NOT a license activation method?

- A. SmartConsole Wizard
- B. Online Activation
- C. License Activation Wizard
- D. Offline Activation

Answer: A

NEW QUESTION 82

- (Exam Topic 1)

Fill in the blank: The command _____ provides the most complete restoration of a R80 configuration.

- A. upgrade_import
- B. cpconfig
- C. fwm dbimport -p <export file>
- D. cpinfo -recover

Answer: A

Explanation:

(Should be "migrate import")

"migrate import" Restores backed up configuration for R80 version, in previous versions the command was " upgrade_import ".

NEW QUESTION 84

- (Exam Topic 1)

Fill in the blank: A _____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

- A. Clientless remote access
- B. Clientless direct access

- C. Client-based remote access
- D. Direct access

Answer: A

Explanation:

Clientless - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.

NEW QUESTION 87

- (Exam Topic 1)

Packages and licenses are loaded from all of these sources EXCEPT

- A. Download Center Web site
- B. UserUpdate
- C. User Center
- D. Check Point DVD

Answer: B

Explanation:

the Download Center web site (packages)

the Check Point DVD (packages)

the User Center (licenses)

by importing a file (packages and licenses)

by running the cplic command line

Packages and licenses are loaded into these repositories from several sources: References:

NEW QUESTION 89

- (Exam Topic 1)

WeBControl Layer has been set up using the settings in the following dialogue:

Consider the following policy and select the BEST answer.

- A. Traffic that does not match any rule in the subpolicy is dropped.
- B. All employees can access only Youtube and Vimeo.
- C. Access to Youtube and Vimeo is allowed only once a day.
- D. Anyone from internal network can access the internet, expect the traffic defined in drop rules 5.2, 5.5 and 5.6.

Answer: D

Explanation:

Policy Layers and Sub-Policies

R80 introduces the concept of layers and sub-policies, allowing you to segment your policy according to your network segments or business units/functions. In addition, you can also assign granular privileges by layer or sub-policy to distribute workload and tasks to the most qualified administrators

With layers, the rule base is organized into a set of security rules. These set of rules or layers, are inspected in the order in which they are defined, allowing control over the rule base flow and the security functionalities that take precedence. If an “accept” action is performed across a layer, the inspection will continue to the next layer. For example, a compliance layer can be created to overlay across a cross-section of rules.

Sub-policies are sets of rules that are created for a specific network segment, branch office or business unit, so if a rule is matched, inspection will continue through this subset of rules before it moves on to the next rule.

Sub-policies and layers can be managed by specific administrators, according to their permissions profiles. This facilitates task delegation and workload distribution.

NEW QUESTION 90

- (Exam Topic 1)

Fill in the blank: The tool ____ generates a R80 Security Gateway configuration report.

- A. infoCP
- B. infoview
- C. cpinfo
- D. fw cpinfo

Answer: C

Explanation:

CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

When contacting Check Point Support, collect the cpinfo files from the Security Management server and Security Gateways involved in your case.

NEW QUESTION 94

- (Exam Topic 1)

When attempting to start a VPN tunnel, in the logs the error 'no proposal chosen' is seen numerous times. No other VPN-related log entries are present. Which phase of the VPN negotiations has failed?

- A. IKE Phase 1
- B. IPSEC Phase 2
- C. IPSEC Phase 1
- D. IKE Phase 2

Answer: D

NEW QUESTION 95

- (Exam Topic 1)

What are the three conflict resolution rules in the Threat Prevention Policy Layers?

- A. Conflict on action, conflict on exception, and conflict on settings
- B. Conflict on scope, conflict on settings, and conflict on exception
- C. Conflict on settings, conflict on address, and conflict on exception
- D. Conflict on action, conflict on destination, and conflict on settings

Answer: C

NEW QUESTION 100

- (Exam Topic 1)

Which policy type has its own Exceptions section?

- A. Threat Prevention
- B. Access Control
- C. Threat Emulation
- D. Desktop Security

Answer: A

Explanation:

The Exceptions Groups pane lets you define exception groups. When necessary, you can create exception groups to use in the Rule Base. An exception group contains one or more defined exceptions. This option facilitates ease-of-use so you do not have to manually define exceptions in multiple rules for commonly required exceptions. You can choose to which rules you want to add exception groups. This means they can be added to some rules and not to others, depending on necessity.

NEW QUESTION 102

- (Exam Topic 1)

What is NOT an advantage of Packet Filtering?

- A. Low Security and No Screening above Network Layer
- B. Application Independence
- C. High Performance
- D. Scalability

Answer: A

Explanation:

Packet Filter Advantages and Disadvantages

NEW QUESTION 107

- (Exam Topic 1)

What are the two high availability modes?

- A. Load Sharing and Legacy
- B. Traditional and New

- C. Active and Standby
- D. New and Legacy

Answer: D

Explanation:

ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

Load Sharing Multicast Mode

Load Sharing Unicast Mode

New High Availability Mode

High Availability Legacy Mode

NEW QUESTION 110

- (Exam Topic 1)

ABC Corp has a new administrator who logs into the Gaia Portal to make some changes. He realizes that even though he has logged in as an administrator, he is unable to make any changes because all configuration options are greyed out as shown in the screenshot image below. What is the likely cause for this?

- A. The Gaia /bin/confd is locked by another administrator from a SmartConsole session.
- B. The database is locked by another administrator SSH session.
- C. The Network address of his computer is in the blocked hosts.
- D. The IP address of his computer is not in the allowed hosts.

Answer: B

Explanation:

There is a lock on top left side of the screen. B is the logical answer.

NEW QUESTION 115

- (Exam Topic 1)

You are the administrator for ABC Corp. You have logged into your R80 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.

What does this mean?

- A. The rule No.6 has been marked for deletion in your Management session.
- B. The rule No.6 has been marked for deletion in another Management session.
- C. The rule No.6 has been marked for editing in your Management session.
- D. The rule No.6 has been marked for editing in another Management session.

Answer: C

NEW QUESTION 116

- (Exam Topic 1)

What are the two types of address translation rules?

- A. Translated packet and untranslated packet
- B. Untranslated packet and manipulated packet
- C. Manipulated packet and original packet
- D. Original packet and translated packet

Answer: D

Explanation:

NAT Rule Base

The NAT Rule Base has two sections that specify how the IP addresses are translated:

Original Packet
Translated Packet References:

NEW QUESTION 119

- (Exam Topic 1)

In which deployment is the security management server and Security Gateway installed on the same appliance?

- A. Bridge Mode
- B. Remote
- C. Standalone
- D. Distributed

Answer: C

Explanation:

Installing Standalone

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

NEW QUESTION 124

- (Exam Topic 1)

Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the Summary screen as in the screenshot below. What as an 'Open Server'?

- A. Check Point software deployed on a non-Check Point appliance.
- B. The Open Server Consortium approved Server Hardware used for the purpose of Security and Availability.
- C. A check Point Management Server deployed using the Open Systems Interconnection (OSI) Server and Security deployment model.
- D. A check Point Management Server software using the Open SSL.

Answer: A

Explanation:

NEW QUESTION 127

- (Exam Topic 2)

What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

- A. degrades performance as the Security Policy grows in size
- B. requires additional Check Point appliances
- C. requires additional software subscription
- D. increases cost

Answer: A

NEW QUESTION 129

- (Exam Topic 2)

Provide very wide coverage for all products and protocols, with noticeable performance impact.

How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

- A. Set High Confidence to Low and Low Confidence to Inactive.
- B. Set the Performance Impact to Medium or lower.
- C. The problem is not with the Threat Prevention Profile
- D. Consider adding more memory to the appliance.
- E. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B

NEW QUESTION 133

- (Exam Topic 2)

You want to reset SIC between smberlin and sgosaka.

In SmartDashboard, you choose sgosaka, Communication, Reset. On sgosaka, you start cpconfig, choose Secure Internal Communication and enter the new SIC Activation Key. The screen reads The SIC was successfully initialized and jumps back to the menu. When trying to establish a connection, instead of a working connection, you receive this error message:

What is the reason for this behavior?

- A. The Gateway was not rebooted, which is necessary to change the SIC key.
- B. You must first initialize the Gateway object in SmartDashboard (i.e., right-click on the object, choose Basic Setup > Initialize).
- C. The Check Point services on the Gateway were not restarted because you are still in the cpconfig utility.
- D. The activation key contains letters that are on different keys on localized keyboard
- E. Therefore, the activation can not be typed in a matching fashion.

Answer: C

NEW QUESTION 138

- (Exam Topic 2)

Which of the following is NOT an element of VPN Simplified Mode and VPN Communities?

- A. "Encrypt" action in the Rule Base
- B. Permanent Tunnels
- C. "VPN" column in the Rule Base
- D. Configuration checkbox "Accept all encrypted traffic"

Answer: A

Explanation:

Migrating from Traditional Mode to Simplified Mode

To migrate from Traditional Mode VPN to Simplified Mode:

1. On the Global Properties > VPN page, select one of these options:

- Simplified mode to all new Firewall Policies
- Traditional or Simplified per new Firewall Policy

2. Click OK.

3. From the R80 SmartConsole Menu, select Manage policies. The Manage Policies window opens.

4. Click New.

The New Policy window opens.

5. Give a name to the new policy and select Access Control.

In the Security Policy Rule Base, a new column marked VPN shows and the Encrypt option is no longer available in the Action column. You are now working in Simplified Mode.

NEW QUESTION 140

- (Exam Topic 2)

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment. Which details she need to fill in System Restore window before she can click OK button and test the backup?

- A. Server, SCP, Username, Password, Path, Comment, Member
- B. Server, TFTP, Username, Password, Path, Comment, All Members
- C. Server, Protocol, Username, Password, Path, Comment, All Members
- D. Server, Protocol, Username, Password, Path, Comment, member

Answer: C

NEW QUESTION 142

- (Exam Topic 2)

What are the three tabs available in SmartView Tracker?

- A. Network & Endpoint, Management, and Active
- B. Network, Endpoint, and Active
- C. Predefined, All Records, Custom Queries
- D. Endpoint, Active, and Custom Queries

Answer: C

NEW QUESTION 145

- (Exam Topic 2)

You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how many often the particular rules match. Where can you see it? Give the BEST answer.

- A. In the SmartView Tracker, if you activate the column Matching Rate.
- B. In SmartReporter, in the section Firewall Blade – Activity > Network Activity with information concerning Top Matched Logged Rules.
- C. SmartReporter provides this information in the section Firewall Blade – Security > Rule Base Analysis with information concerning Top Matched Logged Rules.
- D. It is not possible to see it directl
- E. You can open SmartDashboard and select UserDefined in the Track colum
- F. Afterwards, you need to create your own program with an external counter.

Answer: C

NEW QUESTION 146

- (Exam Topic 2)

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

- A. RADIUS
- B. Remote Access and RADIUS
- C. AD Query
- D. AD Query and Browser-based Authentication

Answer: D

Explanation:

Identity Awareness gets identities from these acquisition sources:

AD Query

Browser-Based Authentication

Endpoint Identity Agent

Terminal Servers Identity Agent

Remote Access

NEW QUESTION 151

- (Exam Topic 2)

Fill in the blanks: The Application Layer Firewalls inspect traffic through the ____ layer(s) of the TCP/IP model and up to and including the ____ layer.

- A. Lower; Application
- B. First two; Internet
- C. First two; Transport

D. Upper; Application

Answer: A

NEW QUESTION 156

- (Exam Topic 2)

Which of the following is NOT an alert option?

- A. SNMP
- B. High alert
- C. Mail
- D. User defined alert

Answer: B

Explanation:

In Action, select:

none - No alert.

log - Sends a log entry to the database.

alert - Opens a pop-up window to your desktop.

mail - Sends a mail alert to your Inbox.

snmptrap - Sends an SNMP alert.

useralert - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert > Alert Commands.

NEW QUESTION 160

- (Exam Topic 2)

Why would an administrator see the message below?

- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- D. A new Policy Package created on the Gateway and transferred to the management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 161

- (Exam Topic 2)

What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.

- A. Search detailed is missing the subnet mask.
- B. There is no object on the database with that name or that IP address.
- C. There is no object on the database with that IP address.
- D. Object does not have a NAT IP address.

Answer: B

NEW QUESTION 165

- (Exam Topic 2)

Which of the following is NOT a back up method?

- A. Save backup
- B. System backup
- C. snapshot
- D. Migrate

Answer: A

Explanation:

The built-in Gaia backup procedures:

Snapshot Management

System Backup (and System Restore)

Save/Show Configuration (and Load Configuration)

Check Point provides three different procedures for backing up (and restoring) the operating system and networking parameters on your appliances.

Snapshot (Revert)

Backup (Restore)

upgrade_export (Migrate) References:

NEW QUESTION 170

- (Exam Topic 2)

In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

- A. Pentagon
- B. Combined
- C. Meshed
- D. Star

Answer: D

Explanation:

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN connections between each Security Gateway. In a Star community, satellites have a VPN connection with the center Security Gateway, but not to each other.

NEW QUESTION 172

- (Exam Topic 2)

Fill in the blank: The ____ software blade enables Application Security policies to allow, block, or limit website access based on user, group, and machine identities.

- A. Application Control
- B. Data Awareness
- C. URL Filtering
- D. Threat Emulation

Answer: A

NEW QUESTION 175

- (Exam Topic 2)

Fill in the blanks: A Check Point software license consists of a ____ and ____.

- A. Software container; software package
- B. Software blade; software container
- C. Software package; signature
- D. Signature; software blade

Answer: B

Explanation:

Check Point's licensing is designed to be scalable and modular. To this end, Check Point offers both predefined packages as well as the ability to custom build a solution tailored to the needs of the Network Administrator. This is accomplished by the use of the following license components:

Software Blades

Container

NEW QUESTION 176

- (Exam Topic 2)

If there is an Accept Implied Policy set to "First", what is the reason Jorge cannot see any logs?

- A. Log Implied Rule was not selected on Global Properties.
- B. Log Implied Rule was not set correctly on the track column on the rules base.
- C. Track log column is set to none.
- D. Track log column is set to Log instead of Full Log.

Answer: A

Explanation:

Implied Rules are configured only on Global Properties.

NEW QUESTION 177

- (Exam Topic 2)

Fill in the blank: A(n) _____ rule is created by an administrator and is located before the first and before last rules in the Rule Base.

- A. Firewall drop
- B. Explicit
- C. Implicit accept
- D. Implicit drop
- E. Implied

Answer: E

Explanation:

This is the order that rules are enforced:

First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.

Explicit Rules: These are rules that you create.

Before Last Implied Rules: These implied rules are applied before the last explicit rule.

Last Explicit Rule: We recommend that you use the Cleanup rule as the last explicit rule.

Last Implied Rules: Implied rules that are configured as Last in Global Properties.

Implied Drop Rule: Drops all packets without logging.

NEW QUESTION 178

- (Exam Topic 2)

Fill in the blanks: A security Policy is created in _____, stored in the _____, and Distributed to the various _____.

- A. Rule base, Security Management Server, Security Gateways
- B. SmartConsole, Security Gateway, Security Management Servers
- C. SmartConsole, Security Management Server, Security Gateways
- D. The Check Point database, SmartConsole, Security Gateways

Answer: C

NEW QUESTION 180

- (Exam Topic 2)

At what point is the Internal Certificate Authority (ICA) created?

- A. Upon creation of a certificate
- B. During the primary Security Management Server installation process.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

Answer: B

Explanation:

Introduction to the ICA

The ICA is a Certificate Authority which is an integral part of the Check Point product suite. It is fully compliant with X.509 standards for both certificates and CRLs. See the relevant X.509 and PKI documentation, as well as RFC 2459 standards for more information. You can read more about Check Point and PKI in the R76 VPN Administration Guide.

The ICA is located on the Security Management server. It is created during the installation process, when the Security Management server is configured.

NEW QUESTION 183

- (Exam Topic 2)

After the initial installation the First Time Configuration Wizard should be run. Select the BEST answer.

- A. First Time Configuration Wizard can be run from the Unified SmartConsole.
- B. First Time Configuration Wizard can be run from the command line or from the WebUI.
- C. First time Configuration Wizard can only be run from the WebUI.
- D. Connection to the internet is required before running the First Time Configuration wizard.

Answer: B

Explanation:

Check Point Security Gateway and Check Point Security Management require running the First Time Configuration Wizard in order to be configured correctly. The First Time Configuration Wizard is available in Gaia Portal and also through CLI.

To invoke the First Time Configuration Wizard through CLI, run the config_system command from the Exp shell.

NEW QUESTION 187

- (Exam Topic 2)

Fill in the blank: Once a license is activated, a _____ should be installed.

- A. License Management file
- B. Security Gateway Contract file
- C. Service Contract file
- D. License Contract file

Answer: C

Explanation:

Service Contract File

Following the activation of the license, a Service Contract File should be installed. This file contains important information about all subscriptions purchased for a specific device and is installed via SmartUpdate. A detailed Explanation: of the Service Contract File can be found in sk33089.

NEW QUESTION 188

- (Exam Topic 2)

You installed Security Management Server on a computer using GAIa in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second GAIa computer, which you plan to ship to another Administrator at a MegaCorp hub office. What is the correct order for pushing SIC certificates to the Gateway before shipping it?

1. Run cpconfig on the Gateway, select Secure Internal Communication, enter the activation key, and reconfirm.
2. Initialize Internal Certificate Authority (ICA) on the Security Management Server.
3. Configure the Gateway object with the host name and IP addresses for the remote site.
4. Click the Communication button in the Gateway object's General screen, enter the activation key, and click Initialize and OK.
5. Install the Security Policy.

- A. 2, 3, 4, 1, 5
- B. 2, 1, 3, 4, 5
- C. 1, 3, 2, 4, 5
- D. 2, 3, 4, 5, 1

Answer: B

NEW QUESTION 189

- (Exam Topic 2)

Choose the SmartLog property that is TRUE.

- A. SmartLog has been an option since release R71.10.
- B. SmartLog is not a Check Point product.
- C. SmartLog and SmartView Tracker are mutually exclusive.
- D. SmartLog is a client of SmartConsole that enables enterprises to centrally track log records and security activity with Google-like search.

Answer: D

NEW QUESTION 193

- (Exam Topic 2)

Which policy type is used to enforce bandwidth and traffic control rules?

- A. Threat Emulation
- B. Access Control
- C. QoS
- D. Threat Prevention

Answer: C

Explanation:

Check Point's QoS Solution

QoS is a policy-based QoS management solution from Check Point Software Technologies Ltd., satisfies your needs for a bandwidth management solution. QoS is a unique, software-only based application that manages traffic end-to-end across networks, by distributing enforcement throughout network hardware and software.

NEW QUESTION 198

- (Exam Topic 2)

Look at the screenshot below. What CLISH command provides this output?

- A. show configuration all
- B. show confd configuration
- C. show confd configuration all
- D. show configuration

Answer: D

NEW QUESTION 199

- (Exam Topic 2)

What is the default method for destination NAT?

- A. Destination side
- B. Source side
- C. Server side

D. Client side

Answer: D

NEW QUESTION 203

- (Exam Topic 2)

Fill in the blank: RADIUS Accounting gets _____ data from requests generated by the accounting client

- A. Destination
- B. Identity
- C. Payload
- D. Location

Answer: B

Explanation:

How RADIUS Accounting Works with Identity Awareness

RADIUS Accounting gets identity data from RADIUS Accounting Requests generated by the RADIUS accounting client.

NEW QUESTION 206

- (Exam Topic 2)

The Captive Portal tool:

- A. Acquires identities from unidentified users.
- B. Is only used for guest user authentication.
- C. Allows access to users already identified.
- D. Is deployed from the Identity Awareness page in the Global Properties settings.

Answer: A

NEW QUESTION 210

- (Exam Topic 2)

The IT Management team is interested in the new features of the Check Point R80 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80 because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

- A. R80 Management contains compatibility packages for managing earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- B. R80 Management requires the separate installation of compatibility hotfix packages for managing the earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- C. R80 Management was designed as a completely different Management system and so can only monitor Check Point Gateways prior to R80.
- D. R80 Management cannot manage earlier versions of Check Point Gateways prior to R80. Only R80 and above Gateways can be manage
- E. Consult the R80 Release Notes for more information.

Answer: A

NEW QUESTION 214

- (Exam Topic 2)

Which information is included in the “Full Log” tracking option, but is not included in the “Log” tracking option?

- A. file attributes
- B. application information
- C. destination port
- D. data type information

Answer: D

Explanation:

Network Log - Generates a log with only basic Firewall information: Source, Destination, Source Port, Destination Port, and Protocol.

Log - Equivalent to the Network Log option, but also includes the application name (for example, Dropbox), and application information (for example, the URL of the Website). This is the default Tracking option.

Full Log - Equivalent to the log option, but also records data for each URL request made.

If suppression is not selected, it generates a complete log (as defined in pre-R80 management).

If suppression is selected, it generates an extended log(as defined in pre-R80 management).

None - Do not generate a log.

NEW QUESTION 215

- (Exam Topic 2)

You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

- A. The POP3 rule is disabled.
- B. POP3 is accepted in Global Properties.
- C. The POP3 rule is hidden.
- D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.

Answer: C

NEW QUESTION 218

- (Exam Topic 2)

Fill in the blank: Licenses can be added to the License and Contract repository _____.

- A. From the User Center, from a file, or manually
- B. From a file, manually, or from SmartView Monitor
- C. Manually, from SmartView Monitor, or from the User Center
- D. From SmartView Monitor, from the User Center, or from a file

Answer: A

NEW QUESTION 222

- (Exam Topic 2)

When using LDAP as an authentication method for Identity Awareness, the query:

- A. Requires client and server side software.
- B. Prompts the user to enter credentials.
- C. Requires administrators to specifically allow LDAP traffic to and from the LDAP Server and the Security Gateway.
- D. Is transparent, requiring no client or server side software, or client intervention.

Answer: D

NEW QUESTION 224

- (Exam Topic 2)

On the following picture an administrator configures Identity Awareness:

After clicking "Next" the above configuration is supported by:

- A. Kerberos SSO which will be working for Active Directory integration
- B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user
- C. Obligatory usage of Captive Portal
- D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication

Answer: B

Explanation:

To enable Identity Awareness:

Log in to R80 SmartConsole.

From the Awareness.

Gateway&s

Servers

view, double-click the Security Gateway on which to enable Identity

On the Network Security tab, select Identity Awareness.

The Identity Awareness

Configuration wizard opens.

Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers

Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).

NEW QUESTION 226

- (Exam Topic 2)

Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAIa, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

- A. She needs to edit /etc/SSHd/SSHd_config and add the Standard Mode account.
- B. She needs to run sysconfig and restart the SSH process.
- C. She needs to edit /etc/scpusers and add the Standard Mode account.
- D. She needs to run cpconfig to enable the ability to SCP files.

Answer: C

NEW QUESTION 227

- (Exam Topic 2)

Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

- A. SmartView Tracker
- B. SmartPortal
- C. SmartUpdate
- D. SmartDashboard

Answer: C

NEW QUESTION 229

- (Exam Topic 2)

Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

- A. Full
- B. Light
- C. Custom
- D. Complete

Answer: A

Explanation:

Endpoint Identity Agents – dedicated client agents installed on users' computers that acquire and report identities to the Security Gateway.

NEW QUESTION 232

- (Exam Topic 2)

The organization's security manager wishes to back up just the Gaia operating system parameters. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries?

- A. show configuration
- B. backup
- C. migrate export
- D. upgrade export

Answer: B

Explanation:

3. System Backup (and System Restore)

System Backup can be used to backup current system configuration. A backup creates a compressed file that contains the Check Point configuration including the networking and operating system parameters, such as routing and interface configuration etc., but unlike a snapshot, it does not include the operating system, product binaries, and hotfixes.

NEW QUESTION 235

- (Exam Topic 3)

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

- A. Threat Emulation
- B. Mobile Access
- C. Mail Transfer Agent
- D. Threat Cloud

Answer: C

NEW QUESTION 237

- (Exam Topic 3)

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

Answer: D

NEW QUESTION 241

- (Exam Topic 3)

Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

- A. Change the Rule Base and install the Policy to all Security Gateways
- B. Block Intruder feature of SmartView Tracker
- C. Intrusion Detection System (IDS) Policy install
- D. SAM – Suspicious Activity Rules feature of SmartView Monitor

Answer: B

NEW QUESTION 243

- (Exam Topic 3)

What is the mechanism behind Threat Extraction?

- A. This is 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 to 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

Answer: D

NEW QUESTION 248

- (Exam Topic 3)

According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

- A. Interoperable Device
- B. Network Node
- C. Externally managed gateway
- D. Gateway

Answer: A

NEW QUESTION 252

- (Exam Topic 3)

The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

- A. Secure Internal Communication (SIC)
- B. Restart Daemons if they fail
- C. Transfer messages between Firewall processes
- D. Pulls application monitoring status

Answer: D

NEW QUESTION 253

- (Exam Topic 3)

Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.

To make this scenario work, the IT administrator must:

- 1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
- 2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
- 3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
- 4) Install policy.

Ms McHanry tries to access the resource but is unable. What should she do?

- A. Have the security administrator select the Action field of the Firewall Rule "Redirect HTTP connections to an authentication (captive) portal".
- B. Have the security administrator reboot the firewall.
- C. Have the security administrator select Any for the Machines tab in the appropriate Access Role.
- D. Install the Identity Awareness agent on her iPad.

Answer: A

NEW QUESTION 258

- (Exam Topic 3)

Your boss wants you to closely monitor an employee suspected of transferring company secrets to the competition. The IT department discovered the suspect installed a WinSCP client in order to use encrypted communication. Which of the following methods is BEST to accomplish this task?

- A. Use SmartView Tracker to follow his actions by filtering log entries that feature the WinSCP destination port
- B. Then, export the corresponding entries to a separate log file for documentation.
- C. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential targets and suspicious protocol
- D. Apply the alert action or customized messaging.
- E. Watch his IP in SmartView Monitor by setting an alert action to any packet that matches your Rule Base and his IP address for inbound and outbound traffic.
- F. Send the suspect an email with a keylogging Trojan attached, to get direct information about his wrongdoings.

Answer: A

NEW QUESTION 261

- (Exam Topic 3)

Which of the below is the MOST correct process to reset SIC from SmartDashboard?

- A. Run cpconfig, and click Reset.
- B. Click the Communication button for the firewall object, then click Reset
- C. Run cpconfig on the gateway and type a new activation key.
- D. Run cpconfig, and select Secure Internal Communication > Change One Time Password.
- E. Click Communication > Reset on the Gateway object, and type a new activation key.

Answer: B

NEW QUESTION 264

- (Exam Topic 3)

A Cleanup rule:

- A. logs connections that would otherwise be dropped without logging by default.
- B. drops packets without logging connections that would otherwise be dropped and logged by default.
- C. logs connections that would otherwise be accepted without logging by default.
- D. drops packets without logging connections that would otherwise be accepted and logged by default.

Answer: A

NEW QUESTION 266

- (Exam Topic 3)

An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).

Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.

If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.

Which of the following is the BEST Explanation: for this behavior?

- A. The setting Log does not capture this level of detail for GR
- B. Set the rule tracking action to Audit since certain types of traffic can only be tracked this way.
- C. The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrupt
- D. Because it is encrypted, the R77 Security Gateway cannot distinguish between GRE session
- E. This is a known issue with GR
- F. Use IPSEC instead of the non-standard GRE protocol for encapsulation.
- G. The Log Server log unification process unifies all log entries from the Security Gateway on a specific connection into only one log entry in the SmartView Tracker
- H. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.
- I. The Log Server is failing to log GRE traffic properly because it is VPN traffic
- J. Disable all VPN configuration to the partner site to enable proper logging.

Answer: C

NEW QUESTION 270

- (Exam Topic 3)

Which command can you use to enable or disable multi-queue per interface?

- A. cpmq set
- B. Cpmqueue set
- C. Cpmq config
- D. Set cpmq enable

Answer: A

NEW QUESTION 272

- (Exam Topic 3)

What is also referred to as Dynamic NAT?

- A. Automatic NAT
- B. Static NAT
- C. Manual NAT
- D. Hide NAT

Answer: D

NEW QUESTION 274

- (Exam Topic 3)

How do you configure the Security Policy to provide users access to the Captive Portal through an external (Internet) interface?

- A. Change the gateway settings to allow Captive Portal access via an external interface.
- B. No action is necessary
- C. This access is available by default.
- D. Change the Identity Awareness settings under Global Properties to allow Captive Policy access on all interfaces.
- E. Change the Identity Awareness settings under Global Properties to allow Captive Policy access for an external interface.

Answer: A

NEW QUESTION 277

- (Exam Topic 3)

Which of these statements describes the Check Point ThreatCloud?

- A. Blocks or limits usage of web applications
- B. Prevents or controls access to web sites based on category
- C. Prevents Cloud vulnerability exploits
- D. A worldwide collaborative security network

Answer: D

NEW QUESTION 281

- (Exam Topic 3)

What is the difference between an event and a log?

- A. Events are generated at gateway according to Event Policy
- B. A log entry becomes an event when it matches any rule defined in Event Policy
- C. Events are collected with SmartWorkflow from Trouble Ticket systems
- D. Logs and Events are synonyms

Answer: B

NEW QUESTION 282

- (Exam Topic 3)

Match the following commands to their correct function. Each command has one function only listed.

- A. C1>F6; C2>F4; C3>F2; C4>F5
- B. C1>F2; C2>F1; C3>F6; C4>F4
- C. C1>F2; C2>F4; C3>F1; C4>F5
- D. C1>F4; C2>F6; C3>F3; C4>F5

Answer: A

NEW QUESTION 286

- (Exam Topic 3)

Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

- A. External-user group
- B. LDAP group
- C. A group with a genetic user
- D. All Users

Answer: B

NEW QUESTION 288

- (Exam Topic 3)

Review the rules. Assume domain UDP is enabled in the implied rules.

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:

- A. can connect to the Internet successfully after being authenticated.
- B. is prompted three times before connecting to the Internet successfully.
- C. can go to the Internet after Telnetting to the client authentication daemon port 259.
- D. can go to the Internet, without being prompted for authentication.

Answer: D

NEW QUESTION 291

- (Exam Topic 3)

Which remote Access Solution is clientless?

- A. Checkpoint Mobile

- B. Endpoint Security Suite
- C. SecuRemote
- D. Mobile Access Portal

Answer: D

NEW QUESTION 292

- (Exam Topic 3)

You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

- A. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0.fws configuration file.
- B. Select Block intruder from the Tools menu in SmartView Tracker.
- C. Create a Suspicious Activity Rule in Smart Monitor.
- D. Add a temporary rule using SmartDashboard and select hide rule.

Answer: C

NEW QUESTION 295

- (Exam Topic 3)

During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

- A. Dropped without sending a negative acknowledgment
- B. Dropped without logs and without sending a negative acknowledgment
- C. Dropped with negative acknowledgment
- D. Dropped with logs and without sending a negative acknowledgment

Answer: D

NEW QUESTION 300

- (Exam Topic 3)

The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the following should you remember?

- A. You can only use the rule for Telnet, FTP, SMTP, and rlogin services.
- B. The Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.
- C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
- D. You can limit the authentication attempts in the User Properties' Authentication tab.

Answer: B

NEW QUESTION 302

- (Exam Topic 3)

What is Consolidation Policy?

- A. The collective name of the Security Policy, Address Translation, and IPS Policies.
- B. The specific Policy written in SmartDashboard to configure which log data is stored in the SmartReporter database.
- C. The collective name of the logs generated by SmartReporter.
- D. A global Policy used to share a common enforcement policy for multiple Security Gateways.

Answer: B

NEW QUESTION 305

- (Exam Topic 3)

As a Security Administrator, you must refresh the Client Authentication authorized time-out every time a new user connection is authorized. How do you do this? Enable the Refreshable Timeout setting:

- A. in the user object's Authentication screen.
- B. in the Gateway object's Authentication screen.
- C. in the Limit tab of the Client Authentication Action Properties screen.
- D. in the Global Properties Authentication screen.

Answer: C

NEW QUESTION 307

- (Exam Topic 3)

You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

- A. Manual copies of the directory \$FWDIR/conf
- B. upgrade_export command
- C. Database Revision Control
- D. GAIa backup utilities

Answer: C

NEW QUESTION 309

- (Exam Topic 3)

Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

- A. Check Point Password
- B. TACACS
- C. LDAP
- D. Windows password

Answer: C

NEW QUESTION 312

- (Exam Topic 3)

Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?

- A. SandBlast Threat Emulation
- B. SandBlast Agent
- C. Check Point Protect
- D. SandBlast Threat Extraction

Answer: D

NEW QUESTION 314

- (Exam Topic 3)

There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?

- A. Using Web Services
- B. Using Mgmt_cli tool
- C. Using CLISH
- D. Using SmartConsole GUI console

Answer: C

NEW QUESTION 316

- (Exam Topic 3)

Which of the following firewall modes DOES NOT allow for Identity Awareness to be deployed?

- A. Bridge
- B. Load Sharing
- C. High Availability
- D. Fail Open

Answer: A

NEW QUESTION 318

- (Exam Topic 3)

VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

- A. 3DES and MD5
- B. Certificates and IPsec
- C. Certificates and pre-shared secret
- D. IPsec and VPN Domains

Answer: C

NEW QUESTION 323

- (Exam Topic 3)

Which set of objects have an Authentication tab?

- A. Templates, Users
- B. Users, Networks
- C. Users, User Group
- D. Networks, Hosts

Answer: A

NEW QUESTION 325

- (Exam Topic 3)

Where would an administrator enable Implied Rules logging?

- A. In Smart Log Rules View
- B. In SmartDashboard on each rule
- C. In Global Properties under Firewall
- D. In Global Properties under log and alert

Answer: B

NEW QUESTION 329

- (Exam Topic 3)

What port is used for communication to the User Center with SmartUpdate?

- A. CPMI 200
- B. TCP 8080
- C. HTTP 80
- D. HTTPS 443

Answer: D

NEW QUESTION 334

- (Exam Topic 3)

Which of the following is a hash algorithm?

- A. 3DES
- B. IDEA
- C. DES
- D. MD5

Answer: D

NEW QUESTION 335

- (Exam Topic 3)

When launching SmartDashboard, what information is required to log into R77?

- A. User Name, Management Server IP, certificate fingerprint file
- B. User Name, Password, Management Server IP
- C. Password, Management Server IP
- D. Password, Management Server IP, LDAP Server IP

Answer: B

NEW QUESTION 338

- (Exam Topic 3)

What is the benefit of Manual NAT over Automatic NAT?

- A. If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy
- B. There is no benefit since Automatic NAT has in any case higher priority over Manual NAT
- C. You have the full control about the priority of the NAT rules
- D. On IPSO and GAIA Gateways, it is handled in a Stateful manner

Answer: C

NEW QUESTION 343

- (Exam Topic 3)

Which tool CANNOT be launched from SmartUpdate R77?

- A. IP Appliance Voyager
- B. snapshot
- C. GAIa WebUI
- D. cpinfo

Answer: B

NEW QUESTION 346

- (Exam Topic 3)

All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

- A. FTP
- B. SMTP
- C. HTTP
- D. RLOGIN

Answer: B

NEW QUESTION 349

- (Exam Topic 3)

Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

- A. Source Address
- B. Destination Address
- C. TCP Acknowledgment Number

D. Source Port

Answer: C

NEW QUESTION 352

- (Exam Topic 3)

You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

- A. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
- B. An office mode address must be obtained by the client.
- C. The SNX client application must be installed on the client.
- D. Active-X must be allowed on the client.

Answer: A

NEW QUESTION 355

- (Exam Topic 4)

How are the backups stored in Chock Point appliances?

- A. Saved as *.tar under /var/log/Cpbackup/backups
- B. Saved as *.tgz under /var/cppbackup
- C. Saved as *.tar under /var/cppbackup
- D. Saved as *.tgz under /var/log/CPbackup/backups

Answer: D

NEW QUESTION 360

- (Exam Topic 4)

To enforce the Security Policy correctly, a Security Gateway requires:

- A. a routing table
- B. awareness of the network topology
- C. a Demilitarized Zone
- D. a Security Policy install

Answer: B

Explanation:

The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

- Correctly enforce the Security Policy.
- Ensure the validity of IP addresses for inbound and outbound traffic.
- Configure a special domain for Virtual Private Networks.

NEW QUESTION 365

- (Exam Topic 4)

R80.10 management server can manage gateways with which versions installed?

- A. Versions R77 and higher
- B. Versions R76 and higher
- C. Versions R75.20 and higher
- D. Version R75 and higher

Answer: B

NEW QUESTION 368

- (Exam Topic 4)

Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

- A. Slow Path
- B. Medium Path
- C. Fast Path
- D. Accelerated Path

Answer: A

NEW QUESTION 373

- (Exam Topic 4)

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

- A. Smart Cloud Services
- B. Load Sharing Mode Services
- C. Threat Agent Solution
- D. Public Cloud Services

Answer: A

NEW QUESTION 377

- (Exam Topic 4)

Which identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

- A. ADQuery
- B. Terminal Servers Endpoint Identity Agent
- C. Endpoint Identity Agent and Browser-Based Authentication
- D. RADIUS and Account Logon

Answer: D

NEW QUESTION 379

- (Exam Topic 4)

Which of the following is NOT a component of Check Point Capsule?

- A. Capsule Docs
- B. Capsule Cloud
- C. Capsule Enterprise
- D. Capsule Workspace

Answer: C

NEW QUESTION 380

- (Exam Topic 4)

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

- A. Next Generation Threat Prevention
- B. Next Generation Threat Emulation
- C. Next Generation Threat Extraction
- D. Next Generation Firewall

Answer: B

NEW QUESTION 382

- (Exam Topic 4)

You want to store the GAIa configuration in a file for later reference. What command should you use?

- A. write mem <filename>
- B. show config -f <filename>
- C. save config -o <filename>
- D. save configuration <filename>

Answer: D

NEW QUESTION 383

- (Exam Topic 4)

Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

- A. SmartManager
- B. SmartConsole
- C. Security Gateway
- D. Security Management Server

Answer: C

NEW QUESTION 387

- (Exam Topic 4)

Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays ____ for the given VPN tunnel.

- A. Down
- B. No Response
- C. Inactive
- D. Failed

Answer: A

NEW QUESTION 389

- (Exam Topic 4)

Which message indicates IKE Phase 2 has completed successfully?

- A. Quick Mode Complete
- B. Aggressive Mode Complete
- C. Main Mode Complete

D. IKE Mode Complete

Answer: A

NEW QUESTION 391

- (Exam Topic 4)

Fill in the blank: In Security Gateways R75 and above, SIC uses _____ for encryption.

- A. AES-128
- B. AES-256
- C. DES
- D. 3DES

Answer: A

NEW QUESTION 396

- (Exam Topic 4)

When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

- A. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
- B. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
- C. The entire Management Database and all sessions and other administrators can connect only as Read-only.
- D. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.

Answer: D

NEW QUESTION 397

- (Exam Topic 4)

What is the Transport layer of the TCP/IP model responsible for?

- A. It transports packets as datagrams along different routes to reach their destination.
- B. It manages the flow of data between two hosts to ensure that the packets are correctly assembled and delivered to the target application.
- C. It defines the protocols that are used to exchange data between networks and how host programs interact with the Application layer.
- D. It deals with all aspects of the physical components of network connectivity and connects with different network types.

Answer: B

NEW QUESTION 399

- (Exam Topic 4)

Using ClusterXL, what statement is true about the Sticky Decision Function?

- A. Can only be changed for Load Sharing implementations
- B. All connections are processed and synchronized by the pivot
- C. Is configured using cpconfig
- D. Is only relevant when using SecureXL

Answer: A

NEW QUESTION 401

- (Exam Topic 4)

What is the purpose of the Clean-up Rule?

- A. To log all traffic that is not explicitly allowed or denied in the Rule Base.
- B. To clean up policies found inconsistent with the compliance blade reports.
- C. To remove all rules that could have a conflict with other rules in the database.
- D. To eliminate duplicate log entries in the Security Gateway

Answer: A

NEW QUESTION 405

- (Exam Topic 4)

Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.

- A. SHA-256
- B. SHA-200
- C. MD5
- D. SHA-128

Answer: A

NEW QUESTION 407

- (Exam Topic 4)

You can see the following graphic:

What is presented on it?

- A. Properties of personal .p12 certificate file issued for user John.
- B. Shared secret properties of John's password.
- C. VPN certificate properties of the John's gateway.
- D. Expired .p12 certificate properties for user John.

Answer: A

NEW QUESTION 409

- (Exam Topic 4)

What is the best sync method in the ClusterXL deployment?

- A. Use 1 cluster + 1st sync
- B. Use 1 dedicated sync interface
- C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
- D. Use 2 clusters + 1st sync + 2nd sync

Answer: B

NEW QUESTION 414

- (Exam Topic 4)

SmartEvent does NOT use which of the following procedures to identify events:

- A. Matching a log against each event definition
- B. Create an event candidate
- C. Matching a log against local exclusions
- D. Matching a log against global exclusions

Answer: C

NEW QUESTION 415

- (Exam Topic 4)

Fill the blank. IT is Best Practice to have a _____ rule at the end of each policy layer.

- A. Explicit Drop
- B. Implied Drop
- C. Explicit Cleanup
- D. Implicit Drop

Answer: A

NEW QUESTION 416

- (Exam Topic 4)

John is using Management HA. Which Smartcenter should be connected to for making changes?

- A. secondary Smartcenter
- B. active Smartcenter
- C. connect virtual IP of Smartcenter HA
- D. primary Smartcenter

Answer: B

NEW QUESTION 417

- (Exam Topic 4)

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the "mgmt_cli" command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia's secure shell (clash)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 420

- (Exam Topic 4)

Which of the following is an authentication method used for Identity Awareness?

- A. SSL
- B. Captive Portal
- C. PKI
- D. RSA

Answer: B

NEW QUESTION 425

- (Exam Topic 4)

Which firewall daemon is responsible for the FW CLI commands?

- A. fwd
- B. fwm
- C. cpm
- D. cpd

Answer: A

NEW QUESTION 426

- (Exam Topic 4)

Fill in the blanks. There are _____ types of software containers _____

- A. Three; security managemen
- B. Security Gateway and endpoint security.
- C. Three; Security Gateway, endpoint Security, and gateway management.
- D. Two; security management and endpoint security
- E. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 431

- (Exam Topic 4)

In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

- A. Accounting
- B. Suppression
- C. Accounting/Suppression
- D. Accounting/Extended

Answer: C

NEW QUESTION 436

- (Exam Topic 4)

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

- A. fw ctl multik dynamic_dispatching on
- B. fw ctl multik dynamic_dispatching set_mode 9
- C. fw ctl multik set_mode 9
- D. fw ctl miltik pq enable

Answer: C

NEW QUESTION 441

- (Exam Topic 4)

You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

- A. restore_backup
- B. import backup
- C. cp_merge
- D. migrate import

Answer: A

NEW QUESTION 445

- (Exam Topic 4)

Fill in the blank; The position of an Implied rule is manipulated in the _____ window

- A. NAT
- B. Firewall
- C. Global Properties
- D. Object Explorer

Answer: C

NEW QUESTION 447

- (Exam Topic 4)

What protocol is specifically used for clustered environments?

- A. Clustered Protocol
- B. Synchronized Cluster Protocol
- C. Control Cluster Protocol
- D. Cluster Control Protocol

Answer: D

NEW QUESTION 448

- (Exam Topic 4)

What is the SOLR database for?

- A. Used for full text search and enables powerful matching capabilities
- B. Writes data to the database and full text search
- C. Serves GUI responsible to transfer request to the DLE server
- D. Enables powerful matching capabilities and writes data to the database

Answer: A

NEW QUESTION 453

- (Exam Topic 4)

When an encrypted packet is decrypted, where does this happen?

- A. Security policy
- B. Inbound chain
- C. Outbound chain
- D. Decryption is not supported

Answer: A

NEW QUESTION 456

- (Exam Topic 4)

Under which file is the proxy arp configuration stored?

- A. \$FWDIR/state/proxy_arp.conf on the management server
- B. \$FWDIR/conf/local.arp on the management server
- C. \$FWDIR/state/_tmp/proxy.arp on the security gateway
- D. \$FWDIR/conf/local.arp on the gateway

Answer: D

NEW QUESTION 460

- (Exam Topic 4)

When using Monitored circuit VRRP, what is a priority delta?

- A. When an interface fails the priority changes to the priority delta
- B. When an interface fails the delta claims the priority
- C. When an interface fails the priority delta is subtracted from the priority
- D. When an interface fails the priority delta decides if the other interfaces takes over

Answer: C

NEW QUESTION 463

- (Exam Topic 4)

Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

- A. Save Policy
- B. install Database
- C. Save Session
- D. install Policy

Answer: D

NEW QUESTION 468

- (Exam Topic 4)

Which repositories are installed on the Security Management Server by SmartUpdate?

- A. License and Update
- B. Package Repository and Licenses
- C. Update and License and Contract
- D. License and Contract and Package Repository

Answer: D

NEW QUESTION 472

- (Exam Topic 4)

What are the three components for Check Point Capsule?

- A. Capsule Docs, Capsule Cloud, Capsule Connect
- B. Capsule Workspace, Capsule Cloud, Capsule Connect

- C. Capsule Workspace, Capsule Docs, Capsule Connect
- D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 476

- (Exam Topic 4)

Fill in the blanks. In _____ NAT, the _____ is translated.

- A. Hide; source
- B. Static; source
- C. Simple; source
- D. Hide; destination

Answer: B

NEW QUESTION 479

- (Exam Topic 4)

Which of the following is NOT a method used by Identity Awareness for acquiring identity?

- A. RADIUS
- B. Active Directory Query
- C. Remote Access
- D. Certificates

Answer: D

NEW QUESTION 484

- (Exam Topic 4)

In the Check Point Security Management Architecture, which component(s) can store logs?

- A. SmartConsole
- B. Security Management Server and Security Gateway
- C. Security Management Server
- D. SmartConsole and Security Management Server

Answer: B

NEW QUESTION 486

- (Exam Topic 4)

Which SmartConsole tab is used to monitor network and security performance?

- A. Manage Seeting
- B. Security Policies
- C. Gateway and Servers
- D. Logs and Monitor

Answer: C

NEW QUESTION 491

- (Exam Topic 4)

Which GUI tool can be used to view and apply Check Point licenses?

- A. cpconfig
- B. Management Command Line
- C. SmartConsole
- D. SmartUpdate

Answer: D

Explanation:

SmartUpdate GUI is the recommended way of managing licenses. References:

NEW QUESTION 492

- (Exam Topic 4)

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

- A. Detects and blocks malware by correlating multiple detection engines before users are affected.
- B. Configure rules to limit the available network bandwidth for specified users or groups.
- C. Use UserCheck to help users understand that certain websites are against the company's security policy.
- D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A

NEW QUESTION 496

- (Exam Topic 4)

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
- B. Threat Extraction always delivers a file and takes less than a second to complete
- C. Threat Emulation never delivers a file that takes less than a second to complete
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Answer: B

NEW QUESTION 498

- (Exam Topic 4)

You want to verify if there are unsaved changes in GAIa that will be lost with a reboot. What command can be used?

- A. show unsaved
- B. show save-state
- C. show configuration diff
- D. show config-state

Answer: D

NEW QUESTION 502

- (Exam Topic 4)

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

- A. ThreatWiki
- B. Whitelist Files
- C. AppWiki
- D. IPS Protections

Answer: A

NEW QUESTION 507

- (Exam Topic 4)

In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

- A. 3rd Party integration of CLI and API for Gateways prior to R80.
- B. A complete CLI and API interface using SSH and custom CPCODE integration.
- C. 3rd Party integration of CLI and API for Management prior to R80.
- D. A complete CLI and API interface for Management with 3rd Party integration.

Answer: B

NEW QUESTION 511

- (Exam Topic 4)

Fill in the blank: An identity server uses a _____ for user authentication.

- A. Shared secret
- B. Certificate
- C. One-time password
- D. Token

Answer: A

NEW QUESTION 516

- (Exam Topic 4)

Which two Identity Awareness commands are used to support identity sharing?

- A. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
- B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
- C. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
- D. Policy Activation Point (PAP) and Policy Decision Point (PDP)

Answer: A

NEW QUESTION 518

- (Exam Topic 4)

Which statement is NOT TRUE about Delta synchronization?

- A. Using UDP Multicast or Broadcast on port 8161
- B. Using UDP Multicast or Broadcast on port 8116
- C. Quicker than Full sync
- D. Transfers changes in the Kernel tables between cluster members

Answer: A

NEW QUESTION 522

- (Exam Topic 4)

Which of the following is the most secure means of authentication?

- A. Password
- B. Certificate
- C. Token
- D. Pre-shared secret

Answer: B

NEW QUESTION 523

- (Exam Topic 4)

Which of the following commands is used to monitor cluster members?

- A. cphaprob state
- B. cphaprob status
- C. cphaprob
- D. cluster state

Answer: A

NEW QUESTION 527

- (Exam Topic 4)

Using R80 Smart Console, what does a “pencil icon” in a rule mean?

- A. I have changed this rule
- B. Someone else has changed this rule
- C. This rule is managed by check point's SOC
- D. This rule can't be changed as it's an implied rule

Answer: A

NEW QUESTION 529

- (Exam Topic 4)

Which path below is available only when CoreXL is enabled?

- A. Slow path
- B. Firewall path
- C. Medium path
- D. Accelerated path

Answer: C

NEW QUESTION 532

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.80 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.80 Product From:

<https://www.2passeasy.com/dumps/156-215.80/>

Money Back Guarantee

156-215.80 Practice Exam Features:

- * 156-215.80 Questions and Answers Updated Frequently
- * 156-215.80 Practice Questions Verified by Expert Senior Certified Staff
- * 156-215.80 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-215.80 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year