

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

```
*****      Select Option      *****

(1)          List all IKE SAs
(2)          List all IPsec SAs
(3)          List all IKE SAs for a given peer (GW) or user (Client)
(4)          List all IPsec SAs for a given peer (GW) or user (Client)
(5)          Delete all IPsec SAs for a given peer (GW)
(6)          Delete all IPsec SAs for a given User (Client)
(7)          Delete all IPsec+IKE SAs for a given peer (GW)
(8)          Delete all IPsec+IKE SAs for a given User (Client)
(9)          Delete all IPsec SAs for ALL peers and users
(0)          Delete all IPsec+IKE SAs for ALL peers and users

(Q)          Quit
```

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 utility allows you to configure the DHCP service on GAIA from the command line?

- A. ifconfig
- B. dhcp_cfg
- C. sysconfig
- D. cpconfig

Answer: C

Explanation:

Sysconfig Configuration Options

	Menu Item	Purpose
7	DHCP Server Configuration	Configure SecurePlatform DHCP Server.
8	DHCP Relay Configuration	Setup DHCP Relay.

NEW QUESTION 4

- (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 5

- (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

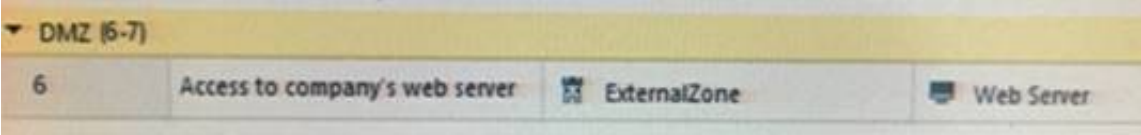
Explanation:

To enable Identity Awareness:
Log in to SmartDashboard.
From the Network Objects tree, expand the Check Poinbtranch.
Double-click the Security Gateway on which to enable Identity Awareness.
In the Software Blades section, select Identity Awarenesosn 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 alof the domain controllers in the organization's Active Directory.

NEW QUESTION 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 1)

Which of the following Automatically Generated Rules NAT rules have the lowest implementation priority?

A. Machine Hide NAT

B. Address Range Hide NAT

C. Network Hide NAT

D. Machine Static NAT

Answer: BC

Explanation:

SmartDashboard organizes the automatic NAT rules in this order:

Static NAT rules for Firewall, or node (computer or server) objects

Hide NAT rules for Firewall, or node objects

Static NAT rules for network or address range objects

Hide NAT rules for network or address range objects

References:

NEW QUESTION 10

- (Exam Topic 1)

DLP and Geo Policy are examples of what type of Policy?

A. Standard Policies

B. Shared Policies

C. Inspection Policies

D. Unified Policies

Answer: B

Explanation:

The Shared policies are installed with the Access Control Policy.

Software Blade	Description
Mobile Access	Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP	Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy	Create a policy for traffic to or from specific geographical or political locations.
HTTPS Policy	The HTTPS Policy allows the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol. To launch the HTTPS Policy, click Manage & Settings > Blades > HTTPS Inspection > Configure in SmartDashboard

NEW QUESTION 10

- (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 14

- (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 16

- (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 20

- (Exam Topic 1)

Which utility shows the security gateway general system information statistics like operating system information and resource usage, and individual software blade statistics of VPN, Identity Awareness and DLP?

- A. cpconfig
B. fw ctl pstat
C. cpview
D. fw ctl multik stat

Answer: C

Explanation:

CPView Utility is a text based built-in utility that can be run ('cpview' command) on Security Gateway / Security Management Server / Multi-Domain Security Management Server. CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway). The data is continuously updated in easy to access views.

NEW QUESTION 24

- (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 29

- (Exam Topic 1)

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

- A. To satellites through center only
B. To center only
C. To center and to other satellites through center
D. To center, or through the center to other satellites, to internet and other VPN targets

Answer: D

Explanation:

On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:

To center and to other Satellites through center; this allows connectivity between Gateways; for example, if the spoke Gateways are DAIP Gateways, and the hub is a Gateway with a static IP address

To center, or through the center to other satellites, to Internet and other VPN targets; this allows connectivity between the Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

NEW QUESTION 30

- (Exam Topic 1)

The following graphic shows:

[illegible]

- A. View from SmartLog for logs initiated from source address 10.1.1.202
- B. View from SmartView Tracker for logs of destination address 10.1.1.202
- C. View from SmartView Tracker for logs initiated from source address 10.1.1.202
- D. View from SmartView Monitor for logs initiated from source address 10.1.1.202

Answer: C

NEW QUESTION 35

- (Exam Topic 1)

Which of the following is NOT an integral part of VPN communication within a network?

- A. VPN key
- B. VPN community
- C. VPN trust entities
- D. VPN domain

Answer: A

Explanation:

VPN key (to not be confused with pre-shared key that is used for authentication).

VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.

VPN Domain - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.

VPN Community - A named collection of VPN domains, each protected by a VPN gateway. References:

http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

NEW QUESTION 36

- (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 38

- (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 41

- (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 45

- (Exam Topic 1)

Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

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

Answer: D

NEW QUESTION 49

- (Exam Topic 1)

When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

- A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
- B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
- C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
- D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Answer: C

NEW QUESTION 50

- (Exam Topic 1)

With which command can you view the running configuration of Gaia-based system.

- A. show conf-active
- B. show configuration active
- C. show configuration
- D. show running-configuration

Answer: C

NEW QUESTION 53

- (Exam Topic 1)

Harriet wants to protect sensitive information from intentional loss when users browse to a specific URL: <https://personal.mymail.com>, which blade will she enable to achieve her goal?

- A. DLP
- B. SSL Inspection
- C. Application Control
- D. URL Filtering

Answer: A

Explanation:

Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies—protecting sensitive corporate information from both intentional and unintentional loss.

NEW QUESTION 56

- (Exam Topic 1)

Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

- A. Block Port Overflow
- B. Local Interface Spoofing
- C. Suspicious Activity Monitoring
- D. Adaptive Threat Prevention

Answer: C

Explanation:

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation

NEW QUESTION 59

- (Exam Topic 1)

Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?

- A. High Availability
- B. Load Sharing Multicast
- C. Load Sharing Pivot
- D. Master/Backup

Answer: B

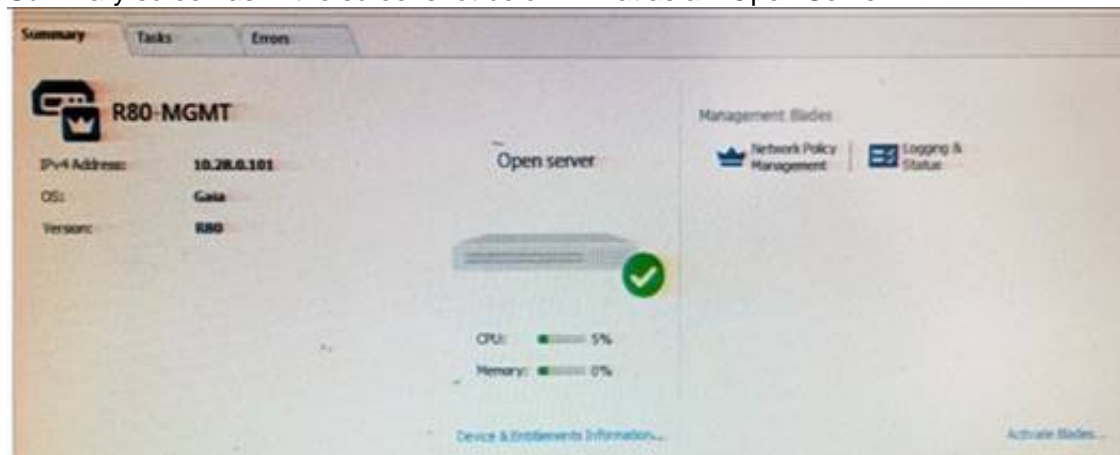
Explanation:

ClusterXL uses the Multicast mechanism to associate the virtual cluster IP addresses with all cluster members. By binding these IP addresses to a Multicast MAC address, it ensures that all packets sent to the cluster, acting as a gateway, will reach all members in the cluster.

NEW QUESTION 60

- (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

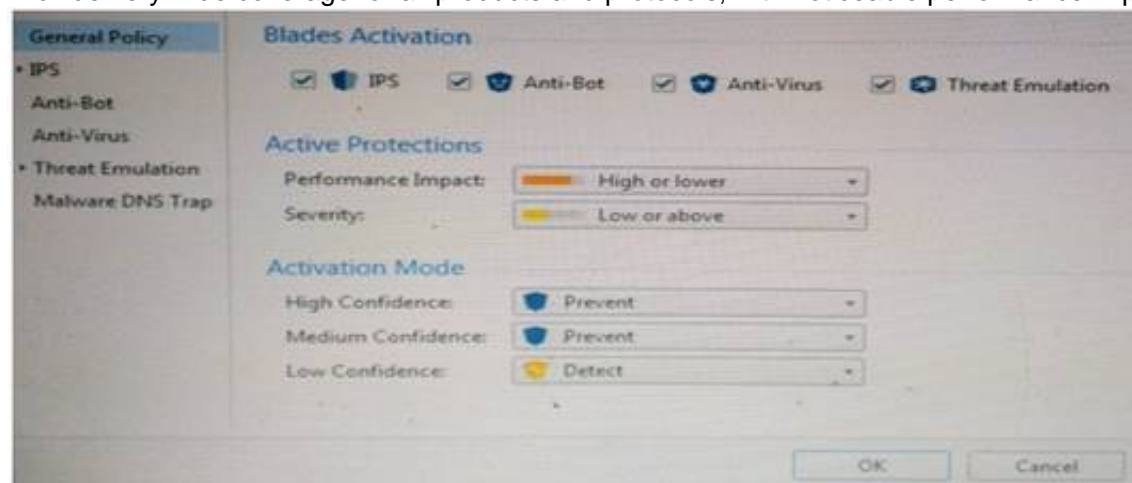
Explanation:

Open Server	Non-Check Point hardware platform that is certified by Check Point as supporting Check Point products. Open Servers allow customers the flexibility of deploying Check Point software on systems which have not been pre-hardened or pre-installed (servers running standard versions of Solaris, Windows, Red Hat Linux).
--------------------	--

NEW QUESTION 62

- (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 Profil
- D. Consider adding more memory to the appliance.
- E. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B

NEW QUESTION 67

- (Exam Topic 2)

In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

- A. Rule 0
- B. Blank field under Rule Number
- C. Rule 1
- D. Cleanup Rule

Answer: A

NEW QUESTION 70

- (Exam Topic 2)

Which of the following is NOT defined by an Access Role object?

- A. Source Network
- B. Source Machine
- C. Source User
- D. Source Server

Answer: D

NEW QUESTION 71

- (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 75

- (Exam Topic 2)

Can a Check Point gateway translate both source IP address and destination IP address in a given packet?

- A. Yes.
- B. No.
- C. Yes, but only when using Automatic NAT.
- D. Yes, but only when using Manual NAT.

Answer: A

NEW QUESTION 78

- (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 83

- (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 84

- (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 85

- (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 88

- (Exam Topic 2)

Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

- A. Firewall
- B. Identity Awareness
- C. Application Control
- D. URL Filtering

Answer: B

Explanation:

Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.

NEW QUESTION 93

- (Exam Topic 2)

Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____.

- A. Firewall policy install
- B. Threat Prevention policy install
- C. Anti-bot policy install
- D. Access Control policy install

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 94

- (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 97

- (Exam Topic 2)

Which command is used to obtain the configuration lock in Gaia?

- A. Lock database override
- B. Unlock database override
- C. Unlock database lock
- D. Lock database user

Answer: A

Explanation:

Obtaining a Configuration Lock
lock database override
unlock database

NEW QUESTION 101

- (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 102

- (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 107

- (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 110

- (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 113

- (Exam Topic 3)

Where do you verify that UserDirectory is enabled?

- A. Verify that Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
- B. Verify that Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked.
- C. Verify that Security Gateway > General Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.
- D. Verify that Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked.

Answer: D

NEW QUESTION 118

- (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 122

- (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 123

- (Exam Topic 3)

Which of the following is NOT a valid option when configuring access for Captive Portal?

- A. From the Internet
- B. Through internal interfaces
- C. Through all interfaces
- D. According to the Firewall Policy

Answer: A

NEW QUESTION 124

- (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 generic user
- D. All Users

Answer: B

NEW QUESTION 126

- (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 130

- (Exam Topic 3)

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

- A. Install appliance TE250X on SpanPort on LAN switch in MTA mode
- B. Install appliance TE250X in standalone mode and setup MTA
- C. You can utilize only Check Point Cloud Services for this scenario
- D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance

Answer: C

NEW QUESTION 135

- (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 140

- (Exam Topic 3)

Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?

- A. Dynamic ID
- B. RADIUS
- C. Username and Password
- D. Certificate

Answer: A

NEW QUESTION 144

- (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 146

- (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 151

- (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 153

- (Exam Topic 3)

You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners. Which SmartConsole application should you use to confirm your suspicion?

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

Answer: D

NEW QUESTION 154

- (Exam Topic 3)

How do you configure an alert in SmartView Monitor?

- A. An alert cannot be configured in SmartView Monitor.
- B. By choosing the Gateway, and Configure Thresholds.
- C. By right-clicking on the Gateway, and selecting Properties.
- D. By right-clicking on the Gateway, and selecting System Information.

Answer: B

NEW QUESTION 158

- (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 162

- (Exam Topic 3)

Identify the API that is not supported by Check Point currently.

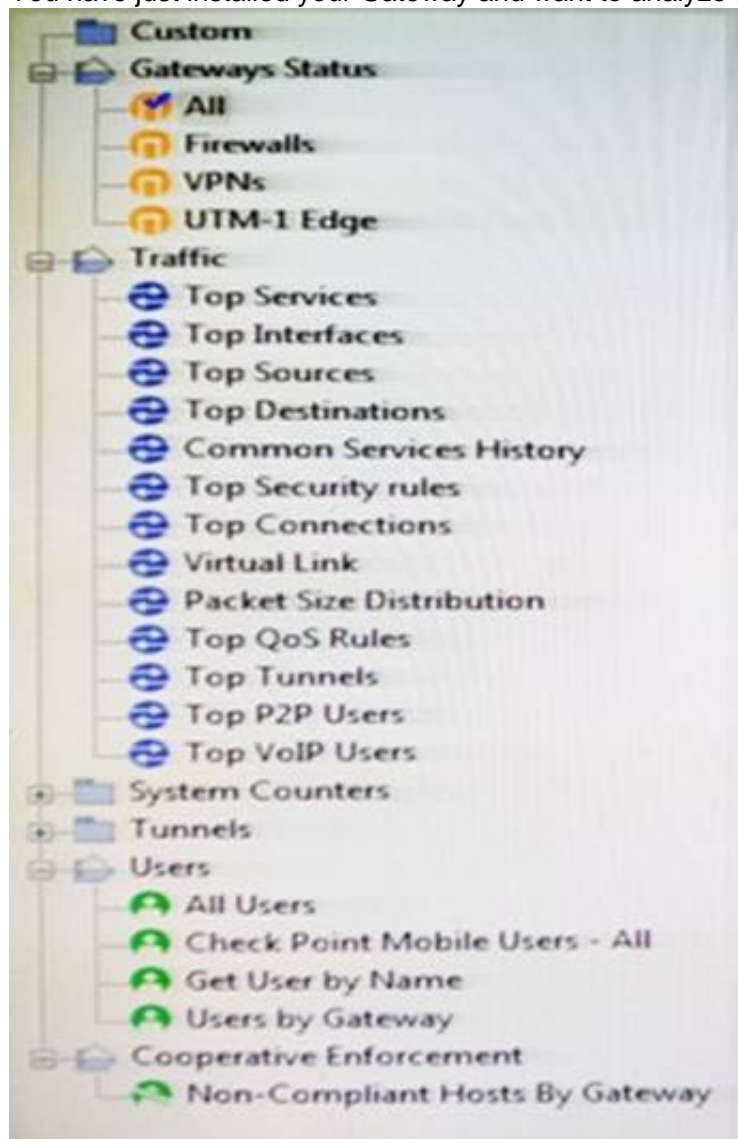
- A. R80 Management API-
- B. Identity Awareness Web Services API
- C. Open REST API
- D. OPSEC SDK

Answer: C

NEW QUESTION 164

- (Exam Topic 3)

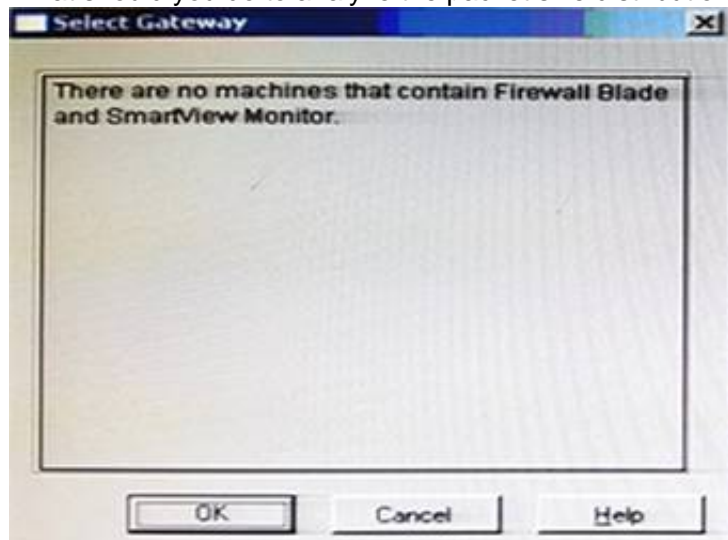
You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.



Unfortunately, you get the message:

“There are no machines that contain Firewall Blade and SmartView Monitor”.

What should you do to analyze the packet size distribution of your traffic? Give the BEST answer.



- A. Purchase the SmartView Monitor license for your Security Management Server.
- B. Enable Monitoring on your Security Management Server.
- C. Purchase the SmartView Monitor license for your Security Gateway.
- D. Enable Monitoring on your Security Gateway.

Answer: D

NEW QUESTION 168

- (Exam Topic 4)

What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?

- A. S
- B. W
- C. C
- D. Space bar

Answer: B

NEW QUESTION 170

- (Exam Topic 4)

The CDT utility supports which of the following?

- A. Major version upgrades to R77.30
- B. Only Jumbo HFA's and hotfixes
- C. Only major version upgrades to R80.10
- D. All upgrades

Answer: D

NEW QUESTION 174

- (Exam Topic 4)

What is the BEST method to deploy identity Awareness for roaming users?

- A. Use Office Mode
- B. Use identity agents
- C. Share user identities between gateways
- D. Use captive portal

Answer: A

NEW QUESTION 177

- (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 181

- (Exam Topic 4)

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265
- B. TCP port 265
- C. UDP port 256
- D. TCP port 256

Answer: B

NEW QUESTION 183

- (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 186

- (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 189

- (Exam Topic 4)

What Identity Agent allows packet tagging and computer authentication?

- A. Endpoint Security Client
- B. Full Agent
- C. Light Agent
- D. System Agent

Answer: B

NEW QUESTION 192

- (Exam Topic 4)

Can multiple administrators connect to a Security Management Server at the same time?

- A. No, only one can be connected
- B. Yes, all administrators can modify a network object at the same time
- C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
- D. Yes, but only one has the right to write

Answer: C

NEW QUESTION 193

- (Exam Topic 4)

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

Answer: D

NEW QUESTION 194

- (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 197

- (Exam Topic 4)

How would you determine the software version from the CLI?

- A. fw ver
- B. fw stat
- C. fw monitor
- D. cpinfo

Answer: A

NEW QUESTION 198

- (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 199

- (Exam Topic 4)

Fill in the blank: To create policy for traffic to or from a particular location, use the_____ .

- A. DLP shared policy
- B. Geo policy shared policy
- C. Mobile Access software blade
- D. HTTPS inspection

Answer: B

Explanation:

Shared Policies

The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages.

Shared policies are installed with the Access Control Policy. Software Blade

Description Mobile Access

Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.

DLP Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.

Geo Policy

Create a policy for traffic to or from specific geographical or political locations. References:

NEW QUESTION 200

- (Exam Topic 4)

When configuring LDAP User Directory integration, Changes applied to a User Directory template are:

- A. Reflected immediately for all users who are using template.
- B. Not reflected for any users unless the local user template is changed.
- C. Reflected for all users who are using that template and if the local user template is changed as well.
- D. Not reflected for any users who are using that template.

Answer: A

Explanation:

The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local.

You can change the User Directory templates. Users

associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.

NEW QUESTION 205

- (Exam Topic 4)

Which command shows the installed licenses?

- A. cplic print
- B. print cplic
- C. fwlic print
- D. show licenses

Answer: A

NEW QUESTION 210

- (Exam Topic 4)

What SmartEvent component creates events?

- A. Consolidation Policy
- B. Correlation Unit
- C. SmartEvent Policy
- D. SmartEvent GUI

Answer: B

NEW QUESTION 214

- (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 216

- (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 218

- (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 220

- (Exam Topic 4)

What is the difference between SSL VPN and IPSec VPN?

- A. IPSec VPN does not require installation of a resident VPN client
- B. SSL VPN requires installation of a resident VPN client
- C. SSL VPN and IPSec VPN are the same
- D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser

Answer: D

NEW QUESTION 223

- (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 224

- (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 226

- (Exam Topic 4)

Which of the following describes how Threat Extraction functions?

- A. Detect threats and provides a detailed report of discovered threats
- B. Proactively detects threats
- C. Delivers file with original content
- D. Delivers PDF versions of original files with active content removed

Answer: B

NEW QUESTION 229

- (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 234

- (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 239

- (Exam Topic 4)

Session unique identifiers are passed to the web api using which http header option?

- A. X-chkp-sid
- B. Accept-Charset
- C. Proxy-Authorization
- D. Application

Answer: C

NEW QUESTION 240

.....

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