

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 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 2

- (Exam Topic 1)

You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R80 gateways.

Answer: A

Explanation:

The most likely reason for the logs data to stop is the low disk space on the logging device, which can be the Management Server or the Gateway Server.

NEW QUESTION 3

- (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 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)

Which of the following is NOT a SecureXL traffic flow?

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

Answer: C

Explanation:

SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:

Slow path - Packets and connections that are inspected by the Firewall and are not processed by SecureXL. Accelerated path - Packets and connections that are offloaded to SecureXL and are not processed by the Firewall.

Medium path - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

NEW QUESTION 6

- (Exam Topic 1)

By default, which port does the WebUI listen on?

- A. 80
- B. 4434
- C. 443
- D. 8080

Answer: C

Explanation:

To configure Security Management Server on Gaia:

Open a browser to the WebUI: <https://Gaia management IP address>

NEW QUESTION 7

- (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 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)

What is the default shell for the command line interface?

- A. Expert
- B. Clish
- C. Admin
- D. Normal

Answer: B

Explanation:

The default shell of the CLI is called clish References:

NEW QUESTION 10

- (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 10

- (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 14

- (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 16

- (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 19

- (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 20

- (Exam Topic 1)

Fill in the blank: The ____ is used to obtain identification and security information about network users.

- A. User Directory
- B. User server
- C. UserCheck
- D. User index

Answer: A

NEW QUESTION 25

- (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 26

- (Exam Topic 1)

Which one of the following is the preferred licensing model? Select the Best answer.

- A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.
- B. Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency of the gateway.
- C. Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.
- D. Central licensing because it ties the package license to the MAC-address of the Security Management Server Mgmt-interface and has no dependency of the gateway.

Answer: B

Explanation:

Central License

A Central License is a license attached to the Security Management server IP address, rather than the gatewa IP address. The benefits of a Central License are:

Only one IP address is needed for all licenses.

A license can be taken from one gateway and given to another.

The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.

NEW QUESTION 31

- (Exam Topic 1)

On the following graphic, you will find layers of policies.

What is a precedence of traffic inspection for the defined policies?

- A. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if implicit Drop Rule drops the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer.
- B. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer
- C. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to Threat Prevention layer and then after accepting the packet it passes to IPS layer.
- D. A packet arrives at the gateway, it is checked against the rules in IPS policy layer and then it comes next to the Network policy layer and then after accepting the packet it passes to Threat Prevention layer.

Answer: B

Explanation:

To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.

For example, when you upgrade to R80 from earlier versions:

Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.

When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.

All layers are evaluated in parallel

When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.

All layers are evaluated in parallel

NEW QUESTION 36

- (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, except 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 40

- (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 45

- (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 46

- (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 48

- (Exam Topic 1)

Where can you trigger a failover of the cluster members?

Log in to Security Gateway CLI and run command clusterXL_admin down.

In SmartView Monitor right-click the Security Gateway member and select Cluster member stop. Log into Security Gateway CLI and run command cphaprob down.

- A. 1, 2, and 3
- B. 2 and 3
- C. 1 and 2
- D. 1 and 3

Answer: C

Explanation:

How to Initiate Failover

NEW QUESTION 50

- (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 51

- (Exam Topic 1)

What is the default time length that Hit Count Data is kept?

- A. 3 month
- B. 4 weeks
- C. 12 months
- D. 6 months

Answer: A

Explanation:

Keep Hit Count data up to - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.

NEW QUESTION 55

- (Exam Topic 1)

Examine the following Rule Base.

What can we infer about the recent changes made to the Rule Base?

- A. Rule 7 was created by the 'admin' administrator in the current session
- B. 8 changes have been made by administrators since the last policy installation
- C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator
- D. Rule 1 and object webserver are locked by another administrator

Answer: D

Explanation:

On top of the print screen there is a number "8" which consists for the number of changes made and not saved. Session Management Toolbar (top of SmartConsole)

NEW QUESTION 59

- (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 61

- (Exam Topic 2)

Mesh and Star are two types of VPN topologies. Which statement below is TRUE about these types of communities?

- A. A star community requires Check Point gateways, as it is a Check Point proprietary technology.
- B. In a star community, satellite gateways cannot communicate with each other.
- C. In a mesh community, member gateways cannot communicate directly with each other.
- D. In a mesh community, all members can create a tunnel with any other member.

Answer: D

NEW QUESTION 66

- (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 69

- (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 73

- (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 77

- (Exam Topic 2)

Which of the following is NOT a set of Regulatory Requirements related to Information Security?

- A. ISO 37001
- B. Sarbanes Oxley (SOX)
- C. HIPPA
- D. PCI

Answer: A

Explanation:

ISO 37001 - Anti-bribery management systems

NEW QUESTION 79

- (Exam Topic 2)

Which of the following is NOT an advantage to using multiple LDAP servers?

- A. You achieve a faster access time by placing LDAP servers containing the database at remote sites
- B. Information on a user is hidden, yet distributed across several servers
- C. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
- D. You gain High Availability by replicating the same information on several servers

Answer: B

NEW QUESTION 84

- (Exam Topic 2)

Which of the following is TRUE about the Check Point Host object?

- A. Check Point Host has no routing ability even if it has more than one interface installed.
- B. When you upgrade to R80 from R77.30 or earlier versions, Check Point Host objects are converted to gateway objects.
- C. Check Point Host is capable of having an IP forwarding mechanism.
- D. Check Point Host can act as a firewall.

Answer: A

Explanation:

A Check Point host is a host with only one interface, on which Check Point software has been installed, and which is managed by the Security Management server. It is not a routing mechanism and is not capable of IP forwarding.

NEW QUESTION 88

- (Exam Topic 2)

Fill in the blanks: A High Availability deployment is referred to as a ____ cluster and a Load Sharing deployment is referred to as a ____ cluster.

- A. Standby/standby; active/active
- B. Active/active; standby/standby
- C. Active/active; active/standby;
- D. Active/standby; active/active

Answer: D

Explanation:

In a High Availability cluster, only one member is active (Active/Standby operation).

ClusterXL Load Sharing distributes traffic within a cluster so that the total throughput of multiple members is increased. In Load Sharing configurations, all

functioning members in the cluster are active, and handle network traffic (Active/Active operation).

NEW QUESTION 90

- (Exam Topic 2)

MyCorp has the following NAT rules. You need to disable the NAT function when Alpha-internal networks try to reach the Google DNS (8.8.8.8) server. What can you do in this case?

- A. Use manual NAT rule to make an exception
- B. Use the NAT settings in the Global Properties
- C. Disable NAT inside the VPN community
- D. Use network exception in the Alpha-internal network object

Answer: D

NEW QUESTION 95

- (Exam Topic 2)

In order to modify Security Policies the administrator can use which of the following tools? Select the BEST answer.

- A. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
- B. SmartConsole and WebUI on the Security Management Server.
- C. mgmt_cli or WebUI on Security Gateway and SmartConsole on the Security Management Server.
- D. SmartConsole or mgmt_cli on any computer where SmartConsole is installed.

Answer: D

NEW QUESTION 96

- (Exam Topic 2)

Study the Rule base and Client Authentication Action properties screen.

After being authenticated by the Security Gateways, a user starts a HTTP connection to a Web site. What happens when the user tries to FTP to another site using the command line? The:

- A. user is prompted for authentication by the Security Gateways again.
- B. FTP data connection is dropped after the user is authenticated successfully.
- C. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client Authentication
- D. FTP connection is dropped by Rule 2.

Answer: C

NEW QUESTION 99

- (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 102

- (Exam Topic 2)

Joey is using the computer with IP address 192.168.20.13. He wants to access web page “www.Check Point.com”, which is hosted on Web server with IP address 203.0.113.111. How many rules on Check Point Firewall are required for this connection?

- A. Two rules – first one for the HTTP traffic and second one for DNS traffic.
- B. Only one rule, because Check Point firewall is a Packet Filtering firewall
- C. Two rules – one for outgoing request and second one for incoming replay.
- D. Only one rule, because Check Point firewall is using Stateful Inspection technology.

Answer: D

NEW QUESTION 106

- (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 107

- (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 108

- (Exam Topic 2)

Administrator wishes to update IPS from SmartConsole by clicking on the option “update now” under the IPS tab. Which device requires internet access for the update to work?

- A. Security Gateway
- B. Device where SmartConsole is installed
- C. SMS
- D. SmartEvent

Answer: B

Explanation:

Updating IPS Manually

You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website. You can only manually update IPS if a proxy is defined in Internet Explorer settings.

To obtain updates of all the latest protections from the IPS website:

Configure the settings for the proxy server in Internet Explorer.

In Microsoft Internet Explorer, open Tools > Internet Options > Connections tab > LAN Settings.

The LAN Settings window opens.

Select Use a proxy server for your LAN.

Configure the IP address and port number for the proxy server.

Click OK.

The settings for the Internet Explorer proxy server are configured.

In the IPS tab, select Download Updates

and click Update Now.

NEW QUESTION 110

- (Exam Topic 2)

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

Answer: B

Explanation:

This chapter gives an introduction to the Gaia command line interface (CLI). The default shell of the CLI is called clish.

NEW QUESTION 112

- (Exam Topic 2)

Anti-Spoofing is typically set up on which object type?

- A. Security Gateway

- B. Host
- C. Security Management object
- D. Network

Answer: A

NEW QUESTION 113

- (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 115

- (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 116

- (Exam Topic 2)

Where can administrator edit a list of trusted SmartConsole clients in R80?

- A. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
- B. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
- C. In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients.
- D. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients, via cpconfig on a Security Gateway.

Answer: C

NEW QUESTION 121

- (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 122

- (Exam Topic 2)

Look at the following screenshot and select the BEST answer.

- A. Clients external to the Security Gateway can download archive files from FTP_Ext server using FTP.
- B. Internal clients can upload and download any-files to FTP_Ext-server using FTP.
- C. Internal clients can upload and download archive-files to FTP_Ext server using FTP.
- D. Clients external to the Security Gateway can upload any files to the FTP_Ext-server using FTP.

Answer: A

NEW QUESTION 126

- (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 127

- (Exam Topic 2)

AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule? Choose the BEST answer.

- A. Rule is locked by AdminA, because the save bottom has not been press.
- B. Rule is locked by AdminA, because an object on that rule is been edited.
- C. Rule is locked by AdminA, and will make it available if session is published.
- D. Rule is locked by AdminA, and if the session is saved, rule will be available

Answer: C

NEW QUESTION 132

- (Exam Topic 2)

You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?

- A. backup
- B. Database Revision
- C. snapshot
- D. migrate export

Answer: C

Explanation:

2. Snapshot Management

The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.

Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.

The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

NEW QUESTION 136

- (Exam Topic 2)

Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?

- A. Create a text-file with mgmt_cli script that creates all objects and policie
- B. Open the file in SmartConsole Command Line to run it.
- C. Create a text-file with Gaia CLI -commands in order to create all objects and policie
- D. Run the file in CLISH with command load configuration.
- E. Create a text-file with DBEDIT script that creates all objects and policie
- F. Run the file in the command line of the management server using command dbedit -f.
- G. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.

Answer: A

Explanation:

Did you know: mgmt_cli can accept csv files as inputs using the --batch option.

The first row should contain the argument names and the rows below it should hold the values for these parameters.

So an equivalent solution to the powershell script could look like this:

data.csv:

mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server>

This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

NEW QUESTION 138

- (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 143

- (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 148

- (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 149

- (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 152

- (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 GRE
- 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 GRE
- 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 156

- (Exam Topic 3)

How many packets does the IKE exchange use for Phase 1 Main Mode?

- A. 12
- B. 1
- C. 3
- D. 6

Answer: D

NEW QUESTION 159

- (Exam Topic 3)

To fully enable Dynamic Dispatcher on a Security Gateway:

- A. run fw ctl multik set_mode 9 in Expert mode and then reboot
- B. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXL menu
- C. Edit /proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot
- D. run fw ctl multik set_mode 1 in Expert mode and then reboot

Answer: A

NEW QUESTION 160

- (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 165

- (Exam Topic 3)

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

- A. SmartView Tracker and SmartView Monitor
- B. SmartLSM and SmartUpdate
- C. SmartDashboard and SmartView Tracker
- D. SmartView Monitor and SmartUpdate

Answer: D

NEW QUESTION 169

- (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 170

- (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 172

- (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 173

- (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 176

- (Exam Topic 3)

Which one of the following is true about Threat Extraction?

- A. Always delivers a file to user
- B. Works on all MS Office, Executables, and PDF files
- C. Can take up to 3 minutes to complete
- D. Delivers file only if no threats found

Answer: B

NEW QUESTION 181

- (Exam Topic 3)

What is the command to see cluster status in cli expert mode?

- A. fw ctl stat
- B. clusterXL stat
- C. clusterXL status
- D. cphaprob stat

Answer: A

NEW QUESTION 182

- (Exam Topic 3)

Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

- A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
- B. mgmt_cli add host name "Server_1" ip_address "10.15.123.10" --format json
- C. mgmt_cli add object-host "Server_1" ip_address "10.15.123.10" --format json
- D. mgmt_cli add object "Server_1" ip_address "10.15.123.10" --format json

Answer: A

NEW QUESTION 186

- (Exam Topic 3)

What is the appropriate default Gaia Portal address?

- A. HTTP://[IPADDRESS]
- B. HTTPS://[IPADDRESS]:8080
- C. HTTPS://[IPADDRESS]:4434
- D. HTTPS://[IPADDRESS]

Answer: D

NEW QUESTION 191

- (Exam Topic 3)

When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

- A. As expert user, issue these commands:# IP link set eth0 down# IP link set eth0 addr 00:0C:29:12:34:56# IP link set eth0 up
- B. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field(conf:(conns:(conn:hwaddr ("00:0C:29:12:34:56"))
- C. As expert user, issue the command:# IP link set eth0 addr 00:0C:29:12:34:56
- D. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.

Answer: C

NEW QUESTION 195

- (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 196

- (Exam Topic 4)

Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made:

- A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of this work.
- B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- C. Tom's changes will be lost since he lost connectivity and he will have to start again.
- D. Tom will have to reboot his SmartConsole computer, clear the cache and restore changes.

Answer: A

NEW QUESTION 197

- (Exam Topic 4)

What is a reason for manual creation of a NAT rule?

- A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
- B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
- C. Network Address Translation is desired for some services, but not for others.
- D. The public IP-address is different from the gateway's external IP

Answer: D

NEW QUESTION 201

- (Exam Topic 4)

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 202

- (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 204

- (Exam Topic 4)

When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

- A. Security Management Server's /home/.fgpt file and is available for future SmartConsole authentications.
- B. Windows registry is available for future Security Management Server authentications.
- C. there is no memory used for saving a fingerprint anyway.
- D. SmartConsole cache is available for future Security Management Server authentications.

Answer: D

NEW QUESTION 209

- (Exam Topic 4)

Fill in the blank: Authentication rules are defined for ____ .

- A. User groups
- B. Users using UserCheck
- C. Individual users
- D. All users in the database

Answer: A

NEW QUESTION 214

- (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 218

- (Exam Topic 4)

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- A. SND is a feature to accelerate multiple SSL VPN connections
- B. SND is an alternative to IPSec Main Mode, using only 3 packets
- C. SND is used to distribute packets among Firewall instances
- D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

NEW QUESTION 219

- (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 223

- (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 228

- (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 232

- (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 234

- (Exam Topic 4)

Which Threat Prevention Profile is not included by default in R80 Management?

- A. Basic – Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance
- B. Optimized – Provides excellent protection for common network products and protocols against recent or popular attacks
- C. Strict – Provides a wide coverage for all products and protocols, with impact on network performance
- D. Recommended – Provides all protection for all common network products and servers, with impact on network performance

Answer: D

NEW QUESTION 237

- (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 241

- (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 244

- (Exam Topic 4)

Please choose correct command syntax to add an “emailserver1” host with IP address 10.50.23.90 using GAIa management CLI?

- A. host name myHost12 ip-address 10.50.23.90
- B. mgmt add host name ip-address 10.50.23.90
- C. add host name emailserver1 ip-address 10.50.23.90
- D. mgmt add host name emailserver1 ip-address 10.50.23.90

Answer: D

NEW QUESTION 247

- (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 248

- (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 249

- (Exam Topic 4)

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 253

- (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 258

- (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 262

- (Exam Topic 4)

When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

- A. Any size
- B. Less than 20GB
- C. More than 10GB and less than 20 GB
- D. At least 20GB

Answer: D

NEW QUESTION 266

- (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 268

- (Exam Topic 4)

What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

- A. ifconfig -a
- B. show interfaces
- C. show interfaces detail
- D. show configuration interface

Answer: D

NEW QUESTION 270

- (Exam Topic 4)

Fill in the blank: Service blades must be attached to a _____. .

- A. Security Gateway
- B. Management container
- C. Management server
- D. Security Gateway container

Answer: A

NEW QUESTION 272

- (Exam Topic 4)

Choose what BEST describes the reason why querying logs now is very fast.

- A. New Smart-1 appliances double the physical memory install
- B. Indexing Engine indexes logs for faster search results
- C. SmartConsole now queries results directly from the Security Gateway
- D. The amount of logs been store is less than the usual in older versions

Answer:

B

NEW QUESTION 276

- (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 278

- (Exam Topic 4)

What Check Point technologies deny or permit network traffic?

- A. Application Control DLP
- B. Packet Filtering, Stateful Inspection, Application Layer Firewall
- C. ACL SandBlast, MPT
- D. IPS, Mobile Threat Protection

Answer: B

NEW QUESTION 280

- (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 284

- (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 288

- (Exam Topic 4)

Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

- A. AES-GCM-256
- B. AES-CBC-256
- C. AES-GCM-128

Answer: B

NEW QUESTION 293

- (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 296

- (Exam Topic 4)

To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

- A. fw ctl set int fwha vmac global param enabled
- B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
- C. cphaprob -a if
- D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Answer: B

NEW QUESTION 297

- (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 300

.....

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