



Check-Point

Exam Questions 156-215.80

Check Point Certified Security Administrator

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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)

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

NEW QUESTION 3

- (Exam Topic 1)

Which product correlates logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

- A. SmartView Monitor
- B. SmartEvent
- C. SmartUpdate
- D. SmartDashboard

Answer: B

Explanation:

SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously.

NEW QUESTION 4

- (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 5

- (Exam Topic 1)

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

Answer: B

Explanation:

To create a new permission profile:

In SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.

Click New Profile.

The New Profile window opens.

Enter a unique name for the profile.

Select a profile type:

Read/Write All - Administrators can make changes

Auditor (Read Only All) - Administrators can see information but cannot make changes

Customized - Configure custom settings

Click OK.

NEW QUESTION 6

- (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 7

- (Exam Topic 1)

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

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

Answer: D

Explanation:

There are different deployment scenarios for Check Point software products.

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

NEW QUESTION 8

- (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 9

- (Exam Topic 1)

Which default user has full read/write access?

- A. Monitor
- B. Altuser
- C. Administrator
- D. Superuser

Answer: C

NEW QUESTION 10

- (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 10

- (Exam Topic 1)

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

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

Answer: D

Explanation:

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

NEW QUESTION 13

- (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 16

- (Exam Topic 1)

When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored

- A. Security Gateway
- B. Check Point user center
- C. Security Management Server
- D. SmartConsole installed device

Answer: C

Explanation:

SmartUpdate installs two repositories on the Security Management server:

License & Contract Repository, which is stored on all platforms in the directory \$FWDIR\conf\.

Package Repository, which is stored:

on Windows machines in C:\SUroot.

on UNIX machines in /var/suroot.

The Package Repository requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the Package Repository.

NEW QUESTION 20

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 22

- (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 27

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 28

- (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 33

- (Exam Topic 1)

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

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

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

Answer: C

Explanation:

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

NEW QUESTION 35

- (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 39

- (Exam Topic 1)

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

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

Answer: A

Explanation:

Access to Web UI Gaia administration interface, initiate a connection from a browser to the default administration IP address: Logging in to the WebUI
Logging in
To log in to the WebUI:
Enter this URL in your browser: <https://<Gaia IP address>>
Enter your user name and password. References:

NEW QUESTION 42

- (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 44

- (Exam Topic 1)

Choose what BEST describes the Policy Layer Traffic Inspection.

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

Answer: B

NEW QUESTION 45

- (Exam Topic 1)

Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

- A. NT domain
- B. SMTP
- C. LDAP
- D. SecurID

Answer: C

NEW QUESTION 47

- (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 51

- (Exam Topic 1)

The following graphic shows:

- 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 53

- (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 58

- (Exam Topic 1)

Fill in the blanks: VPN gateways authenticate using _____ and _____.

- A. Passwords; tokens
- B. Certificates; pre-shared secrets
- C. Certificates; passwords
- D. Tokens; pre-shared secrets

Answer: B

Explanation:

VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

NEW QUESTION 60

- (Exam Topic 1)

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CPApp

Answer: B

Explanation:

AppWiki Application Classification Library

AppWiki enables application scanning and detection of more than 5,000 distinct applications and over 300,000 Web 2.0 widgets including instant messaging, social networking, video streaming, VoIP, games and more.

NEW QUESTION 65

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 66

- (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 69

- (Exam Topic 1)

In R80, Unified Policy is a combination of

- A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.
- B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- D. Access control policy, QoS Policy, Desktop Security Policy and VPN policy.

Answer: D

Explanation:

D is the best answer given the choices. Unified Policy

In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

Firewall and VPN
Application Control and URL Filtering
Identity Awareness
Data Awareness
Mobile Access
Security Zones

NEW QUESTION 71

- (Exam Topic 1)

If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

- A. Publish or discard the session.
- B. Revert the session.
- C. Save and install the Policy.
- D. Delete older versions of database.

Answer: A

Explanation:

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

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.

When you select Install Policy, you are prompted to publish all unpublished changes. You cannot install a policy if the included changes are not published.

NEW QUESTION 75

- (Exam Topic 1)

In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

- A. Display policies and logs on the administrator's workstation.
- B. Verify and compile Security Policies.
- C. Processing and sending alerts such as SNMP traps and email notifications.
- D. Store firewall logs to hard drive storage.

Answer: A

NEW QUESTION 79

- (Exam Topic 1)

In R80 spoofing is defined as a method of:

- A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
- B. Hiding your firewall from unauthorized users.
- C. Detecting people using false or wrong authentication logins
- D. Making packets appear as if they come from an authorized IP address.

Answer: D

Explanation:

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

NEW QUESTION 80

- (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 83

- (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 84

- (Exam Topic 1)

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

Consider the following policy and select the BEST answer.

- A. Traffic that does not match any rule in the subpolicy is dropped.
- B. All employees can access only Youtube and Vimeo.
- C. Access to Youtube and Vimeo is allowed only once a day.

D. Anyone from internal network can access the internet, expect the traffic defined in drop rules 5.2, 5.5 and 5.6.

Answer: D

Explanation:

Policy Layers and Sub-Policies

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

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

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

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

NEW QUESTION 89

- (Exam Topic 1)

Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when ____.

- A. The license is attached to the wrong Security Gateway
- B. The existing license expires
- C. The license is upgraded
- D. The IP address of the Security Management or Security Gateway has changed

Answer: A

Explanation:

There is no need to generate new license in this situation, just need to detach license from wrong Security Gateway and attach it to the right one.

NEW QUESTION 92

- (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 97

- (Exam Topic 1)

What are the two high availability modes?

- A. Load Sharing and Legacy
- B. Traditional and New
- C. Active and Standby
- D. New and Legacy

Answer: D

Explanation:

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

Load Sharing Multicast Mode

Load Sharing Unicast Mode

New High Availability Mode

High Availability Legacy Mode

NEW QUESTION 100

- (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 101

- (Exam Topic 1)

To optimize Rule Base efficiency, the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.

Answer: C

Explanation:

It is logical that if lesser rules are checked for the matched rule to be found the lesser CPU cycles the device is using. Checkpoint match a session from the first rule on top till the last on the bottom.

NEW QUESTION 102

- (Exam Topic 1)

Which feature is NOT provided by all Check Point Mobile Access solutions?

- A. Support for IPv6
- B. Granular access control
- C. Strong user authentication
- D. Secure connectivity

Answer: A

Explanation:

Types of Solutions

Enterprise-grade, secure connectivity to corporate resources.

Strong user authentication.

Granular access control. References:

NEW QUESTION 103

- (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 107

- (Exam Topic 1)

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

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

Answer: B

Explanation:

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

NEW QUESTION 112

- (Exam Topic 1)

Which Threat Prevention Software Blade provides comprehensive protection against malicious and unwanted network traffic, focusing on application and server vulnerabilities?

- A. Anti-Virus
- B. IPS
- C. Anti-Spam
- D. Anti-bot

Answer: B

Explanation:

The IPS Software Blade provides a complete Intrusion Prevention System security solution, providing comprehensive network protection against malicious and unwanted network traffic, including:

- Malware attacks
- Dos and DDoS attacks
- Application and server vulnerabilities
- Insider threats
- Unwanted application traffic, including IM and P2P

NEW QUESTION 116

- (Exam Topic 1)

What are the two types of address translation rules?

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

Answer: D

Explanation:

NAT Rule Base

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

- Original Packet
- Translated Packet References:

NEW QUESTION 119

- (Exam Topic 1)

Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.

Where can the administrator check for more information on these errors?

- A. The Log and Monitor section in SmartConsole
- B. The Validations section in SmartConsole
- C. The Objects section in SmartConsole
- D. The Policies section in SmartConsole

Answer: B

Explanation:

Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.

To publish, you must fix the errors.

NEW QUESTION 124

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Installing Standalone

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

NEW QUESTION 126

- (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 131

- (Exam Topic 2)

What statement is true regarding Visitor Mode?

- A. VPN authentication and encrypted traffic are tunneled through port TCP 443.
- B. Only ESP traffic is tunneled through port TCP 443.
- C. Only Main mode and Quick mode traffic are tunneled on TCP port 443.
- D. All VPN traffic is tunneled through UDP port 4500.

Answer: A

NEW QUESTION 132

- (Exam Topic 2)

Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is ____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

- A. Accept; redirect
- B. Accept; drop
- C. Redirect; drop
- D. Drop; accept

Answer: D

NEW QUESTION 136

- (Exam Topic 2)

What are the three tabs available in SmartView Tracker?

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

Answer: C

NEW QUESTION 139

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 142

- (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 147

- (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 152

- (Exam Topic 2)

Where do we need to reset the SIC on a gateway object?

- A. SmartDashboard > Edit Gateway Object > General Properties > Communication
- B. SmartUpdate > Edit Security Management Server Object > SIC
- C. SmartUpdate > Edit Gateway Object > Communication
- D. SmartDashboard > Edit Security Management Server Object > SIC

Answer: A

NEW QUESTION 154

- (Exam Topic 2)

Which of the following is NOT an alert option?

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

Answer: B

Explanation:

In Action, select:

none - No alert.

log - Sends a log entry to the database.

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

mail - Sends a mail alert to your Inbox.

snmptrap - Sends an SNMP alert.

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

NEW QUESTION 156

- (Exam Topic 2)

Why would an administrator see the message below?

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

Answer: B

NEW QUESTION 157

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 160

- (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 165

- (Exam Topic 2)

Which of the following is NOT a VPN routing option available in a star community?

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

Answer: A

Explanation:

SmartConsole

For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:

On the Star Community window, in the:

Center Gateways section, select the Security Gateway that functions as the "Hub".

Satellite Gateways section, select Security Gateways as the "spokes", or satellites.

On the VPN Routing page, Enable VPN routing for satellites section, select one of these options:

To center and to other Satellites through center - This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security 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 Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.

Create an appropriate Access Control Policy rule.

NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.

The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.

NEW QUESTION 166

- (Exam Topic 2)

You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the "Select additional profile that will be able edit this layer" you do not see anything. What is the most likely cause of this problem? Select the BEST answer.

- A. "Edit layers by Software Blades" is unselected in the Permission Profile
- B. There are no permission profiles available and you need to create one first.
- C. All permission profiles are in use.
- D. "Edit layers by selected profiles in a layer editor" is unselected in the Permission profile.

Answer: B

NEW QUESTION 169

- (Exam Topic 2)

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, gateway policy permits access only from John's desktop which is assigned an IP address 10.0.0.19 via DHCP.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but the limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to move around the organization and continue to have access to the HR Web Server. To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

- A. John should install the identity Awareness Agent
- B. The firewall admin should install the Security Policy
- C. John should lock and unlock the computer
- D. Investigate this as a network connectivity issue

Answer: C

NEW QUESTION 173

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 175

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

Software Blades
Container

NEW QUESTION 179

- (Exam Topic 2)

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

- A. Firewall drop

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

Answer: E

Explanation:

This is the order that rules are enforced:

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

Explicit Rules: These are rules that you create.

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

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

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

Implied Drop Rule: Drops all packets without logging.

NEW QUESTION 181

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 185

- (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 186

- (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 191

- (Exam Topic 2)

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

- A. Firewall
- B. Application Control
- C. Anti-spam and Email Security
- D. Antivirus

Answer: D

Explanation:

The enhanced Check Point Antivirus Software Blade uses real-time virus signatures and anomaly-based protections from ThreatCloud™, the first collaborative network to fight cybercrime, to detect and block malware at the gateway before users are affected.

NEW QUESTION 193

- (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 194

- (Exam Topic 2)

Choose the SmartLog property that is TRUE.

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

Answer: D

NEW QUESTION 199

- (Exam Topic 2)

Choose what BEST describes users on Gaia Platform.

- A. There is one default user that cannot be deleted.
- B. There are two default users and one cannot be deleted.
- C. There is one default user that can be deleted.
- D. There are two default users that cannot be deleted and one SmartConsole Administrator.

Answer: B

Explanation:

These users are created by default and cannot be deleted:

admin — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user has a User ID of 0, and therefore has all of the privileges of a root user.

monitor — Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.

NEW QUESTION 203

- (Exam Topic 2)

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.
- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server

Answer: D

Explanation:

Users

Use the WebUI and CLI to manage user accounts. You can:

Add users to your Gaia system.

Edit the home directory of the user.

Edit the default shell for a user.

Give a password to a user.

Give privileges to users.

NEW QUESTION 204

- (Exam Topic 2)

Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

- A. When Joe logs in, Bob will be log out automatically.
- B. Since they both are log in on different interfaces, they both will be able to make changes.
- C. If Joe tries to make changes, he won't, database will be locked.
- D. Bob will be prompt that Joe logged in.

Answer: C

NEW QUESTION 205

- (Exam Topic 2)

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

- A. Threat Emulation
- B. Access Control

- C. QoS
- D. Threat Prevention

Answer: C

Explanation:

Check Point's QoS Solution

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

NEW QUESTION 207

- (Exam Topic 2)

What is the default method for destination NAT?

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

Answer: D

NEW QUESTION 210

- (Exam Topic 2)

Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?

- A. The two algorithms do not have the same key length and so don't work together
- B. You will get the error... No proposal chosen...
- C. All is fine as the longest key length has been chosen for encrypting the data and a shorter key length for higher performance for setting up the tunnel.
- D. Only 128 bit keys are used for phase 1 keys which are protecting phase 2, so the longer key length in phase 2 only costs performance and does not add security due to a shorter key in phase 1.
- E. All is fine and can be used as is.

Answer: C

NEW QUESTION 213

- (Exam Topic 2)

What happens if the identity of a user is known?

- A. If the user credentials do not match an Access Role, the system displays the Captive Portal.
- B. If the user credentials do not match an Access Role, the system displays a sandbox.
- C. If the user credentials do not match an Access Role, the traffic is automatically dropped.
- D. If the user credentials match an Access Role, the rule is applied and traffic is accepted or dropped based on the defined action.

Answer: D

NEW QUESTION 214

- (Exam Topic 2)

NAT can NOT be configured on which of the following objects?

- A. HTTP Logical Server
- B. Gateway
- C. Address Range
- D. Host

Answer: A

NEW QUESTION 215

- (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 219

- (Exam Topic 2)

What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

- A. show interface (interface) –chain
- B. tcpdump
- C. tcpdump /snoop
- D. fw monitor

Answer: D

NEW QUESTION 222

- (Exam Topic 2)

Message digests use which of the following?

- A. DES and RC4
- B. IDEA and RC4
- C. SSL and MD4
- D. SHA-1 and MD5

Answer: D

NEW QUESTION 223

- (Exam Topic 2)

The most important part of a site-to-site VPN deployment is the ____.

- A. Internet
- B. Remote users
- C. Encrypted VPN tunnel
- D. VPN gateways

Answer: C

Explanation:

Site to Site VPN

The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

NEW QUESTION 225

- (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 227

- (Exam Topic 2)

Which authentication scheme requires a user to possess a token?

- A. TACACS
- B. SecurID
- C. Check Point password
- D. RADIUS

Answer: B

Explanation:

SecurID
SecurID requires users to both possess a token authenticator and to supply a PIN or password References:

NEW QUESTION 230

- (Exam Topic 2)

Which of the following statements accurately describes the command snapshot?

- A. snapshot creates a full OS-level backup, including network-interface data, Check Point production information, and configuration settings of a GAiA Security Gateway.
- B. snapshot creates a Security Management Server full system-level backup on any OS
- C. snapshot stores only the system-configuration settings on the Gateway
- D. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server

Answer: A

NEW QUESTION 231

- (Exam Topic 2)

The fw monitor utility is used to troubleshoot which of the following problems?

- A. Phase two key negotiation
- B. Address translation
- C. Log Consolidation Engine
- D. User data base corruption

Answer: B

NEW QUESTION 232

- (Exam Topic 2)

On the following picture an administrator configures Identity Awareness:

After clicking “Next” the above configuration is supported by:

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

Answer: B

Explanation:

To enable Identity Awareness:

Log in to R80 SmartConsole.

From the Awareness.

Gateway&s

Servers

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

On the Network Security tab, select Identity Awareness.

The Identity Awareness

Configuration wizard opens.

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

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

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

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

NEW QUESTION 233

- (Exam Topic 2)

Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.

- A. Shared policy packages
- B. Shared policies
- C. Concurrent policy packages
- D. Concurrent policies

Answer: A

NEW QUESTION 238

- (Exam Topic 2)

How many users can have read/write access in Gaia at one time?

- A. Infinite
- B. One
- C. Three
- D. Two

Answer: B

NEW QUESTION 242

- (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 246

- (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 248

- (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 252

- (Exam Topic 3)

In what way are SSL VPN and IPSec VPN different?

- A. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
- B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
- C. IPSec VPN does not support two factor authentication, SSL VPN does support this
- D. IPSec VPN uses an additional virtual adapter, SSL VPN uses the client network adapter only

Answer: D

NEW QUESTION 254

- (Exam Topic 3)

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

- A. Change the Rule Base and install the Policy to all Security Gateways

- B. Block Intruder feature of SmartView Tracker
- C. Intrusion Detection System (IDS) Policy install
- D. SAM – Suspicious Activity Rules feature of SmartView Monitor

Answer: B

NEW QUESTION 257

- (Exam Topic 3)

Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?

- A. There is no traffic queue to be handled
- B. Several NICs can use one traffic queue by one CPU
- C. Each NIC has several traffic queues that are handled by multiple CPU cores
- D. Each NIC has one traffic queue that is handled by one CPU

Answer: C

NEW QUESTION 261

- (Exam Topic 3)

As you review this Security Policy, what changes could you make to accommodate Rule 4?

- A. Remove the service HTTP from the column Service in Rule 4.
- B. Modify the column VPN in Rule 2 to limit access to specific traffic.
- C. Nothing at all
- D. Modify the columns Source or Destination in Rule 4

Answer: B

NEW QUESTION 262

- (Exam Topic 3)

The Firewall kernel is replicated multiple times, therefore:

- A. The Firewall kernel only touches the packet if the connection is accelerated
- B. The Firewall can run different policies per core
- C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
- D. The Firewall can run the same policy on all cores

Answer: D

NEW QUESTION 264

- (Exam Topic 3)

What component of R80 Management is used for indexing?

- A. DBSync
- B. API Server
- C. fwm
- D. SOLR

Answer: D

NEW QUESTION 266

- (Exam Topic 3)

Which is the correct order of a log flow processed by SmartEvent components:

- A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
- B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
- C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
- D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

NEW QUESTION 268

- (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 270

- (Exam Topic 3)

The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them?

- A. Six times per day
- B. Seven times per day
- C. Every two hours
- D. Every three hours

Answer: D

NEW QUESTION 274

- (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 276

- (Exam Topic 3)

Choose the correct statement regarding Implicit Rules.

- A. To edit the Implicit rules you go to: Launch Button > Policy > Global Properties > Firewall.
- B. Implied rules are fixed rules that you cannot change.
- C. You can directly edit the Implicit rules by double-clicking on a specific Implicit rule.
- D. You can edit the Implicit rules but only if requested by Check Point support personnel.

Answer: A

NEW QUESTION 278

- (Exam Topic 3)

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

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

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

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

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

Answer: C

NEW QUESTION 281

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 284

- (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 286

- (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 290

- (Exam Topic 3)

Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

- A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
- B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
- C. SmartView Tracker, CPINFO, SmartUpdate
- D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Answer: C

NEW QUESTION 292

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 296

- (Exam Topic 3)

Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except:

- A. Create new dashboards to manage 3rd party task
- B. Create products that use and enhance 3rd party solutions
- C. Execute automated scripts to perform common tasks
- D. Create products that use and enhance the Check Point Solution

Answer: A

NEW QUESTION 301

- (Exam Topic 3)

The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

- A. There is a virus found
- B. Traffic is still allowed but not accelerated
- C. The connection required a Security server
- D. Acceleration is not enabled
- E. The traffic is originating from the gateway itself

Answer: D

NEW QUESTION 302

- (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 307

- (Exam Topic 3)

Which command can you use to verify the number of active concurrent connections?

- A. fw conn all
- B. fw ctl pst pstat
- C. show all connections
- D. show connections

Answer: B

NEW QUESTION 311

- (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 316

- (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 317

- (Exam Topic 3)

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

- A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
- B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
- C. Mail, Block Source, Block Destination, External Script, SNMP Trap
- D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

NEW QUESTION 321

- (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 322

- (Exam Topic 3)

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

- A. Secure Internal Communications (SIC) not configured for the object.
- B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
- C. Anti-spoofing not configured on the interfaces on the Gateway object.
- D. A Gateway object created using the Check Point > Secure Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Answer: B

NEW QUESTION 323

- (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 328

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 332

- (Exam Topic 3)

You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

- A. You checked the cache password on desktop option in Global Properties.
- B. Another rule that accepts HTTP without authentication exists in the Rule Base.
- C. You have forgotten to place the User Authentication Rule before the Stealth Rule.
- D. Users must use the SecuRemote Client, to use the User Authentication Rule.

Answer: B

NEW QUESTION 337

- (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 338

- (Exam Topic 3)

You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities should you do first?

- A. Create a new logical-server object to represent your partner's CA
- B. Exchange exported CA keys and use them to create a new server object to represent your partner's Certificate Authority (CA)
- C. Manually import your partner's Certificate Revocation List.
- D. Manually import your partner's Access Control List.

Answer: B

NEW QUESTION 341

- (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 344

- (Exam Topic 3)

Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

- A. Blue > add local backup
- B. Expert@Blue#add local backing
- C. Blue > set backup local
- D. Blue > add backup local

Answer: D

NEW QUESTION 346

- (Exam Topic 3)

While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?

- 1) Select Active Mode tab in SmartView Tracker.
- 2) Select Tools > Block Intruder.
- 3) Select Log Viewing tab in SmartView Tracker.
- 4) Set Blocking Timeout value to 60 minutes.
- 5) Highlight connection that should be blocked.

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

Answer: C

NEW QUESTION 348

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 350

- (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 351

- (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 352

- (Exam Topic 3)

You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After a while, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

- A. Run fwm dbexport -1 filename
- B. Restore the databas
- C. Then, run fwm dbimport -1 filename to import the users.
- D. Run fwm_dbexport to export the user databas
- E. Select restore the entire database in the Database Revision scree
- F. Then, run fwm_dbimport.
- G. Restore the entire database, except the user database, and then create the new user and user group.
- H. Restore the entire database, except the user database.

Answer: D

NEW QUESTION 353

- (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 suspicious?

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

Answer: D

NEW QUESTION 354

- (Exam Topic 3)

Which of the following is NOT an attribute of packer acceleration?

- A. Source address
- B. Protocol
- C. Destination port
- D. Application Awareness

Answer: D

NEW QUESTION 358

- (Exam Topic 3)

You are about to integrate RSA SecurID users into the Check Point infrastructure. What kind of users are to be defined via SmartDashboard?

- A. A group with generic user
- B. All users
- C. LDAP Account Unit Group
- D. Internal user Group

Answer: A

NEW QUESTION 362

- (Exam Topic 3)

According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added?

A(n):

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

Answer: C

NEW QUESTION 367

- (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 370

- (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 375

- (Exam Topic 3)

What is the benefit of Manual NAT over Automatic NAT?

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

Answer: C

NEW QUESTION 379

- (Exam Topic 3)

Which tool CANNOT be launched from SmartUpdate R77?

- A. IP Appliance Voyager
- B. snapshot

- C. GAIa WebUI
- D. cpinfo

Answer: B

NEW QUESTION 383

- (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 387

- (Exam Topic 3)

When defining QoS global properties, which option below is not valid?

- A. Weight
- B. Authenticated timeout
- C. Schedule
- D. Rate

Answer: C

NEW QUESTION 390

- (Exam Topic 3)

What are types of Check Point APIs available currently as part of R80.10 code?

- A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API
- B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
- C. OSE API, OPSEC SDK API, Threat Prevention API and Policy Editor API
- D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

NEW QUESTION 395

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 398

- (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 400

- (Exam Topic 4)

How are the backups stored in Chock Point appliances?

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

Answer: D

NEW QUESTION 404

- (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 409

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 412

- (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 415

- (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 417

- (Exam Topic 4)

Which one of the following is TRUE?

- A. Ordered policy is a sub-policy within another policy
- B. One policy can be either inline or ordered, but not both
- C. Inline layer can be defined as a rule action
- D. Pre-R80 Gateways do not support ordered layers

Answer: C

NEW QUESTION 419

- (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 422

- (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 426

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 430

- (Exam Topic 4)

What does it mean if Deyra sees the gateway status

Choose the BEST answer.

- A. SmartCenter Server cannot reach this Security Gateway
- B. There is a blade reporting a problem
- C. VPN software blade is reporting a malfunction
- D. Security Gateway s MGNT NIC card is disconnected

Answer: A

NEW QUESTION 435

- (Exam Topic 4)

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R80 configuration, clean install R80.10 and import the configuration
- B. CPUSE online upgrade
- C. CPUSE offline upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 436

- (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 438

- (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 439

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 441

- (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 446

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 450

- (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 453

- (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 454

- (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 455

- (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 457

- (Exam Topic 4)

The SIC Status “Unknown” means

- A. There is connection between the gateway and Security Management Server but it is not trusted.
- B. The secure communication is established.
- C. There is no connection between the gateway and Security Management Server.
- D. The Security Management Server can contact the gateway, but cannot establish SIC.

Answer: C
Explanation: SICStatus

Explanation:

After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

Communicating - The secure communication is established.

Unknown - There is no connection between the gateway and Security Management Server.

Not Communicating - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

NEW QUESTION 458

- (Exam Topic 4)

Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Answer: B

NEW QUESTION 459

- (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 460

- (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 464

- (Exam Topic 4)

What is the best sync method in the ClusterXL deployment?

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

Answer: B

NEW QUESTION 465

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 468

- (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. T 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 472

- (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 475

- (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 477

- (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 479

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 480

- (Exam Topic 4)

When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

- A. Distributed
- B. Standalone
- C. Bridge

Answer: A

NEW QUESTION 483

- (Exam Topic 4)

Which deployment adds a Security Gateway to an existing environment without changing IP routing?

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

Answer: B

NEW QUESTION 485

- (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 489

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 494

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 497

- (Exam Topic 4)

How many sessions can be opened on the Management Server at the same time?

- A. Unlimited, One per each licensed Gateway
- B. One
- C. Unlimited, Multiple per administrator
- D. Unlimited, One per administrator

Answer: D

NEW QUESTION 502

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 506

- (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 509

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 510

- (Exam Topic 4)

What are the three components for Check Point Capsule?

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

D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 513

- (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 514

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 518

- (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 522

- (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 523

- (Exam Topic 4)

True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

- A. False, this feature has to be enabled in the Global Properties.
- B. True, every administrator works in a session that is independent of the other administrators.
- C. True, every administrator works on a different database that is independent of the other administrators.
- D. False, only one administrator can login with write permission.

Answer: B

Explanation:

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

NEW QUESTION 528

- (Exam Topic 4)

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- A. Symmetric routing
- B. Failovers
- C. Asymmetric routing
- D. Anti-Spoofing

Answer: B

NEW QUESTION 529

- (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 531

- (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 536

- (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 541

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 546

- (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 549

- (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 553

- (Exam Topic 4)

Which of the following is NOT a valid deployment option for R80?

- A. All-in-one (stand-alone)
- B. Log Server
- C. SmartEvent
- D. Multi-domain management server

Answer: D

NEW QUESTION 558

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 562

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 567

- (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 571

- (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 576

- (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 579

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 582

- (Exam Topic 4)

Which path below is available only when CoreXL is enabled?

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

Answer: C

NEW QUESTION 585

- (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 586

.....

Relate Links

100% Pass Your 156-215.80 Exam with Exam Bible Prep Materials

<https://www.exambible.com/156-215.80-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>