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

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

Answer: D

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

NEW QUESTION 4
- (Exam Topic 1)
You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

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

Answer: A

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

NEW QUESTION 5
- (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 6
- (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 7
- (Exam Topic 1)
What does ExternalZone represent in the presented rule?

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

Answer: B

Explanation:
Configuring Interfaces
Configure the Security Gateway 80 interfaces in the Interfaces tab in the Security Gateway window. To configure the interfaces:
From the Devices window, double-click the Security Gateway 80.
The Security Gateway
window opens.
Select the Interfaces tab.
Select Use the following settings. The interface settings open.
Select the interface and click Edit.
The Edit window opens.
From the IP Assignment section, configure the IP address of the interface:
Select Static IP.
Enter the IP address and subnet mask for the interface.
In Security Zone, select Wireless, DMS, External, or Internal. Security zone is a type of zone, created by a bridge to easily create segments, while maintaining IP addresses and router configurations. Security zones let you choose if to enable or not the firewall between segments.
References:

NEW QUESTION 8
- (Exam Topic 1)
Which default user has full read/write access?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
Which command is used to add users to or from existing roles?

A. Add rba user <User Name> roles <List>
B. Add rba user <User Name>
C. Add user <User Name> roles <List>
D. Add user <User Name>

Answer: A

Explanation:
Configuring Roles - CLI (rba)

NEW QUESTION 10
- (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 10
- (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 11
- (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 13
- (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 14
- (Exam Topic 1)
What is the purpose of Captive Portal?

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

Answer: C

Explanation:

Captive Portal – a simple method that authenticates users through a web interface before granting them access to Intranet resources. When users try to access a protected resource, they get a web page that
must be filled out to continue.
Reference : https://www.checkpoint.com/products/identity-awareness-software-blade/

NEW QUESTION 19
- (Exam Topic 1)
What will be the effect of running the following command on the Security Management Server?

A. Remove the installed Security Policy.
B. Remove the local ACL lists.
C. No effect.
D. Reset SIC on all gateways.

Answer: A

Explanation:
This command uninstall actual security policy (already installed) References:

NEW QUESTION 20
- (Exam Topic 1)
View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.

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

Answer: B

Explanation:
Administrator Collaboration
More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.
When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.
To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

NEW QUESTION 23
- (Exam Topic 1)
Review the following screenshot and select the BEST answer.

A. Data Center Layer is an inline layer in the Access Control Policy.
B. By default all layers are shared with all policies.
C. If a connection is dropped in Network Layer, it will not be matched against the rules in Data Center Layer.
D. If a connection is accepted in Network-layer, it will not be matched against the rules in Data Center Layer.

Answer: C

NEW QUESTION 27
- (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 28
- (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 30
- (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 33
- (Exam Topic 1)
Which application should you use to install a contract file?

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

Answer: C

Explanation:
Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 /
Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.
Open SmartUpdate and from the Launch Menu select 'Licenses & Contracts' -> 'Update Contracts' -> 'From File...' and provide the path to the file you have downloaded in Step #3:

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

NEW QUESTION 37
- (Exam Topic 1)
Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

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

Answer: D

Explanation:
On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:
To center and to other Satellites through center; this allows connectivity between Gateways; for example, if the spoke Gateways are DAIP Gateways, and the hub is a Gateway with a static IP address
To center, or through the center to other satellites, to Internet and other VPN targets; this allows connectivity between the Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

NEW QUESTION 42
- (Exam Topic 1)
Fill in the blank: The ____ is used to obtain identification and security information about network users.

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

Answer: A

NEW QUESTION 44
- (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 47
- (Exam Topic 1)
Which of the following is NOT an integral part of VPN communication within a network?

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

Answer: A

Explanation:
VPN key (to not be confused with pre-shared key that is used for authentication).
VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.
VPN Domain - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.
VPN Community - A named collection of VPN domains, each protected by a VPN gateway. References:
http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

NEW QUESTION 48
- (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 49
- (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 50
- (Exam Topic 1)
What is the order of NAT priorities?

A. Static NAT, IP pool NAT, hide NAT
B. IP pool NAT, static NAT, hide NAT
C. Static NAT, automatic NAT, hide NAT
D. Static NAT, hide NAT, IP pool NAT

Answer: A

Explanation:
The order of NAT priorities is:
Static NAT
IP Pool NAT
Hide NAT
Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

NEW QUESTION 53
- (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 57
- (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 58
- (Exam Topic 1)
Fill in the blank: The command _____ provides the most complete restoration of a R80 configuration.

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

Answer: A

Explanation:
(Should be "migrate import")
"migrate import" Restores backed up configuration for R80 version, in previous versions the command was " upgrade_import ".

NEW QUESTION 60
- (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 63
- (Exam Topic 1)
Which one of the following is the preferred licensing model? Select the Best answer.

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

Answer: B

Explanation:
Central License
A Central License is a license attached to the Security Management server IP address, rather than the gatewa IP address. The benefits of a Central License are:
Only one IP address is needed for all licenses.
A license can be taken from one gateway and given to another.
The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.

NEW QUESTION 66
- (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 70
- (Exam Topic 1)
Fill in the blank: A ____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

A. Clientless remote access
B. Clientless direct access
C. Client-based remote access
D. Direct access

Answer: A

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

NEW QUESTION 73
- (Exam Topic 1)
On the following graphic, you will find layers of policies.

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

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 76
- (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 77
- (Exam Topic 1)
The security Gateway is installed on GAiA R80 The default port for the WEB User Interface is ____.

A. TCP 18211
B. TCP 257
C. TCP 4433
D. TCP 443

Answer: D

NEW QUESTION 79
- (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 84
- (Exam Topic 1)
Which policy type has its own Exceptions section?

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

Answer: A

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

on necessity.

NEW QUESTION 88
- (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 90
- (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 93
- (Exam Topic 1)
What is the default time length that Hit Count Data is kept?

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

Answer: A

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

NEW QUESTION 98
- (Exam Topic 1)
Examine the following Rule Base.

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

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

Answer: D

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

NEW QUESTION 99
- (Exam Topic 1)
Which Threat Prevention Software Blade provides comprehensive 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 103
- (Exam Topic 1)
You are the administrator for ABC Corp. You have logged into your R80 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.

What does this mean?

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

Answer: C

NEW QUESTION 104
- (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 106
- (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 109
- (Exam Topic 1)
Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the Summary screen as in the screenshot below. What as an 'Open Server'?

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

Answer: A

Explanation:

NEW QUESTION 111
- (Exam Topic 2)
What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

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

Answer: A

NEW QUESTION 116
- (Exam Topic 2)
You want to reset SIC between smberlin and sgosaka.

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

What is the reason for this behavior?

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

Answer: C

NEW QUESTION 120
- (Exam Topic 2)
Which of the following is NOT an element of VPN Simplified Mode and VPN Communities?

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

Answer: A

Explanation:
Migrating from Traditional Mode to Simplified Mode
To migrate from Traditional Mode VPN to Simplified Mode:

1. On the Global Properties > VPN page, select one of these options:
• Simplified mode to all new Firewall Policies
• Traditional or Simplified per new Firewall Policy
2. Click OK.
3. From the R80 SmartConsole Menu, select Manage policies. The Manage Policies window opens.
4. Click New.
The New Policy window opens.
5. Give a name to the new policy and select Access Control.
In the Security Policy Rule Base, a new column marked VPN shows and the Encrypt option is no longer available in the Action column. You are now working in Simplified Mode.

NEW QUESTION 123
- (Exam Topic 2)
Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment. Which details she need to fill in System Restore window before she can click OK button and test the backup?

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

Answer: C

NEW QUESTION 127
- (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 128
- (Exam Topic 2)
Which of the following is NOT defined by an Access Role object?

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

Answer: D

NEW QUESTION 129
- (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 133
- (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 bythe Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 137
- (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 138
- (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 Communitywindow, 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 141
- (Exam Topic 2)
Fill in the blank: A ____ is used by a VPN gateway to send traffic as if it were a physical interface.

A. VPN Tunnel Interface
B. VPN community
C. VPN router
D. VPN interface

Answer: A

Explanation:
Route Based VPN
VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it were a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols.

NEW QUESTION 142
- (Exam Topic 2)
Which of these components does NOT require a Security Gateway R77 license?

A. Security Management Server
B. Check Point Gateway
C. SmartConsole
D. SmartUpdate upgrading/patching

Answer: C

NEW QUESTION 147
- (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 152
- (Exam Topic 2)
Which of the following is TRUE about the Check Point Host object?

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

Answer: A

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

NEW QUESTION 154
- (Exam Topic 2)
What action can be performed from SmartUpdate R77?

A. upgrade_export
B. fw stat -1
C. cpinfo
D. remote_uninstall_verifier

Answer: C

NEW QUESTION 158
- (Exam Topic 2)
If there is an Accept Implied Policy set to “First”, what is the reason Jorge cannot see any logs?

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

Answer: A

Explanation:
Implied Rules are configured only on Global Properties.

NEW QUESTION 159
- (Exam Topic 2)
Fill in the blanks: A High Availability deployment is referred to as a ____ cluster and a Load Sharing deployment is referred to as a _____ cluster.

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

Answer: D

Explanation:
In a High Availability cluster, only one member is active (Active/Standby operation).
ClusterXL Load Sharing distributes traffic within a cluster so that the total throughput of multiple members is increased. In Load Sharing configurations, all functioning members in the cluster are active, and handle network traffic (Active/Active operation).

NEW QUESTION 162
- (Exam Topic 2)
MyCorp has the following NAT rules. You need to disable the NAT function when Alpha-internal networks try to reach the Google DNS (8.8.8.8) server.
What can you do in this case?

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

Answer: D

NEW QUESTION 164
- (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 169
- (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 174
- (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 175
- (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 176
- (Exam Topic 2)
Fill in the blank: Once a license is activated, a ____ should be installed.

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

Answer: C

Explanation:

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

NEW QUESTION 177
- (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 182
- (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 184
- (Exam Topic 2)
Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

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

Answer: B

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

NEW QUESTION 189
- (Exam Topic 2)
Choose the SmartLog property that is TRUE.

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

Answer: D

NEW QUESTION 191
- (Exam Topic 2)
Which feature in R77 permits blocking specific IP addresses for a specified time period?

A. Suspicious Activity Monitoring
B. HTTP Methods
C. Local Interface Spoofing
D. Block Port Overflow

Answer: A

NEW QUESTION 192
- (Exam Topic 2)
There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic in the morning. FW_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW_B became active. After an hour, FW_A’s interface issues were resolved and it became operational. When it re-joins the cluster, will it become active automatically?

A. No, since “maintain current active cluster member” option on the cluster object properties is enabled by default
B. No, since “maintain current active cluster member” option is enabled by default on the Global Properties

C. Yes, since “Switch to higher priority cluster member” option on the cluster object properties is enabled by default
D. Yes, since “Switch to higher priority cluster member” option is enabled by default on the Global Properties

Answer: A

Explanation:
What Happens When a Security Gateway Recovers?
In a Load Sharing configuration, when the failed Security Gateway in a cluster recovers, all connections are redistributed among all active members. High Availability and Load Sharing in ClusterXL ClusterXL Administration Guide R77 Versions | 31 In a High Availability configuration, when the failed Security Gateway in a cluster recovers, the recovery method depends on the configured cluster setting. The options are:
• Maintain Current Active Security Gateway means that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events.
• Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

NEW QUESTION 194
- (Exam Topic 2)
Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____.

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

Answer: B

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

NEW QUESTION 199
- (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 200
- (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 203
- (Exam Topic 2)
The Captive Portal tool:

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

Answer: A

NEW QUESTION 207
- (Exam Topic 2)
Where can administrator edit a list of trusted SmartConsole clients in R80?

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

Answer: C

NEW QUESTION 211
- (Exam Topic 2)
Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

A. SmartMonitor
B. SmartView Web Application
C. SmartReporter
D. SmartTracker

Answer: B

Explanation:
Event Analysis with SmartEvent
The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.

NEW QUESTION 213
- (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 218
- (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 220
- (Exam Topic 2)
In the R80 SmartConsole, on which tab are Permissions and Administrators defined?

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

Answer: C

NEW QUESTION 223
- (Exam Topic 2)
Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as _____

A. UserCheck

B. User Directory
C. User Administration
D. User Center

Answer: B

Explanation:
Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.

NEW QUESTION 228
- (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 233
- (Exam Topic 2)
AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule? Choose the BEST answer.

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

Answer: C

NEW QUESTION 235
- (Exam Topic 2)
Fill in the blank: Licenses can be added to the License and Contract repository _____.

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

Answer: A

NEW QUESTION 236
- (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 241
- (Exam Topic 2)
Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAiA, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

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

Answer: C

NEW QUESTION 243
- (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 248
- (Exam Topic 2)
What port is used for delivering logs from the gateway to the management server?

A. Port 258
B. Port 18209
C. Port 257
D. Port 981

Answer: C

NEW QUESTION 250
- (Exam Topic 2)
R80 Security Management Server can be installed on which of the following operating systems?

A. Gaia only
B. Gaia, SPLAT, Windows Server only
C. Gaia, SPLAT, Windows Server and IPSO only
D. Gaia and SPLAT only

Answer: A

Explanation:
R80 can be installed only on GAIA OS.
Supported Check Point Installations All R80 servers are supported on the Gaia Operating System:
• Security Management Server
• Multi-Domain Security Management Server
• Log Server
• Multi-Domain Log Server
• SmartEvent Server

NEW QUESTION 252
- (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 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 256
- (Exam Topic 3)
What is the mechanism behind Threat Extraction?

A. This is a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender
B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient
C. This is a new mechanism to identify the IP address of the sender of malicious codes and to put it into the SAM database (Suspicious Activity Monitoring).
D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast

Answer: D

NEW QUESTION 257
- (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 260
- (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 261
- (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 263
- (Exam Topic 3)
Which of the below is the MOST correct process to reset SIC from SmartDashboard?

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

Answer: B

NEW QUESTION 268
- (Exam Topic 3)
A Cleanup rule:

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

Answer: A

NEW QUESTION 272
- (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 277
- (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 278
- (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 279
- (Exam Topic 3)
What is also referred to as Dynamic NAT?

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

Answer: D

NEW QUESTION 282
- (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 286
- (Exam Topic 3)
How do you configure the Security Policy to provide uses 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 necessar
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 288
- (Exam Topic 3)
Which of the following actions do NOT take place in IKE Phase 1?

A. Peers agree on encryption method.
B. Diffie-Hellman key is combined with the key material to produce the symmetrical IPsec key.
C. Peers agree on integrity method.
D. Each side generates a session key from its private key and peer's public key.

Answer: B

NEW QUESTION 289
- (Exam Topic 3)
Match the following commands to their correct function. Each command has one function only listed.

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

Answer: A

NEW QUESTION 290
- (Exam Topic 3)
You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

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

Answer: D

NEW QUESTION 293
- (Exam Topic 3)
Review the rules. Assume domain UDP is enabled in the implied rules.
What happens when a user from the internal network tries to browse to the internet using HTTP? The user:

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

Answer: D

NEW QUESTION 295
- (Exam Topic 3)
Which of the following is NOT an option for internal network definition of Anti-spoofing?

A. Specific – derived from a selected object
B. Route-based – derived from gateway routing table
C. Network defined by the interface IP and Net Mask
D. Not-defined

Answer: B

NEW QUESTION 297
- (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 298
- (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 301
- (Exam Topic 3)
Which of the following uses the same key to decrypt as it does to encrypt?

A. Asymmetric encryption
B. Dynamic encryption
C. Certificate-based encryption
D. Symmetric encryption

Answer: D

NEW QUESTION 303
- (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 306
- (Exam Topic 3)
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, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.
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 that 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 desktop with a static IP (10.0.0.19). 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 installs the policy.
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.
3) Changes from static IP address to DHCP for the client PC.
What should John request when he cannot access the web server from his laptop?

A. John should lock and unlock his computer
B. Investigate this as a network connectivity issue
C. The access should be changed to authenticate the user instead of the PC
D. John should install the Identity Awareness Agent

Answer: C

NEW QUESTION 307
- (Exam Topic 3)
What happens if the identity of a user is known?

A. If the user credentials do not match an Access Role, the traffic is automatically dropped.
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 gateway moves onto the next rule.
D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

Answer: C

NEW QUESTION 308
- (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 311
- (Exam Topic 3)
As a Security Administrator, you must refresh the Client Authentication authorized time-out every time a new user connection is authorized. How do you do this?
Enable the Refreshable Timeout setting:

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

Answer: C

NEW QUESTION 312
- (Exam Topic 3)
On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

A. 18210
B. 18184
C. 257
D. 18191

Answer: B

NEW QUESTION 315
- (Exam Topic 3)
What is the Manual Client Authentication TELNET port?

A. 23
B. 264
C. 900
D. 259

Answer: D

NEW QUESTION 316
- (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 317
- (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 sh 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 320
- (Exam Topic 3)
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

A. XlateDst
B. XlateSPort
C. XlateDPort
D. XlateSrc

Answer: B

NEW QUESTION 321
- (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 324
- (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 328
- (Exam Topic 3)
Where would an administrator enable Implied Rules logging?

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

Answer: B

NEW QUESTION 329
- (Exam Topic 3)
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 330
- (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 333
- (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 338
- (Exam Topic 3)
Which NAT rules are prioritized first?

A. Post-Automatic/Manual NAT rules
B. Manual/Pre-Automatic NAT
C. Automatic Hide NAT
D. Automatic Static NAT

Answer: B

NEW QUESTION 339
- (Exam Topic 3)
Which of the following is a hash algorithm?

A. 3DES
B. IDEA

C. DES
D. MD5

Answer: D

NEW QUESTION 340
- (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 345
- (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 349
- (Exam Topic 3)
What is the purpose of Priority Delta in VRRP?

A. When a box is up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fails, Effective Priority = Priority - Priority Delta
D. When a box fails, Effective Priority = Priority - Priority Delta

Answer: C

NEW QUESTION 353
- (Exam Topic 3)
All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

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

Answer: B

NEW QUESTION 356
- (Exam Topic 3)
Identify the API that is not supported by Check Point currently.

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

Answer: C

NEW QUESTION 360
- (Exam Topic 3)
What happens when you run the command: fw sam -J src [Source IP Address]?

A. Connections from the specified source are blocked without the need to change the Security Policy.
B. Connections to the specified target are blocked without the need to change the Security Policy.
C. Connections to and from the specified target are blocked without the need to change the Security Policy.
D. Connections to and from the specified target are blocked with the need to change the Security Policy.

Answer: A

NEW QUESTION 365
- (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 367
- (Exam Topic 4)
To enforce the Security Policy correctly, a Security Gateway requires:

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

Answer: B

Explanation:
The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:
Correctly enforce the Security Policy.
Ensure the validity of IP addresses for inbound and outbound traffic.
Configure a special domain for Virtual Private Networks.

NEW QUESTION 372
- (Exam Topic 4)
Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rule
B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
D. Time object to a rule to make the rule active only during specified times.
E. Sub Policies are sets of rules that can be created and attached to specific rule
F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 376
- (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 378
- (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 381
- (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 384
- (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 388
- (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 389
- (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 392
- (Exam Topic 4)
The _____ software blade package uses CPU-level and OS-level sandboxing in order to delect and block malware.

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

Answer: B

NEW QUESTION 397
- (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 401
- (Exam Topic 4)
Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

What is the possible Explanation: for this?

A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
B. Another administrator is logged into the Management and currently editing the DNS Rule.
C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.
D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Answer: B

NEW QUESTION 403
- (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 408
- (Exam Topic 4)
If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
B. Change the Standby Security Management Server to Active.
C. Change the Active Security Management Server to Standby.
D. Manually synchronize the Active and Standby Security Management Servers.

Answer: A

NEW QUESTION 410
- (Exam Topic 4)
Which back up utility captures the most information and tends to create the largest archives?

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

Answer: B

NEW QUESTION 411
- (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 415
- (Exam Topic 4)
Fill in the blank: In Security Gateways R75 and above, SIC uses _____ for encryption.

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

Answer: A

NEW QUESTION 420
- (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 422
- (Exam Topic 4)
Which of the following is NOT an option to calculate the traffic direction?

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

Answer: D

NEW QUESTION 426
- (Exam Topic 4)
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

A. Go to clash-Run cpstop | Run cpstart

B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
C. Administrator does not need to perform any tas
D. Check Point will make use of the newly installed CPU and Cores
E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer: B

NEW QUESTION 430
- (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 435
- (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 437
- (Exam Topic 4)
SmartEvent does NOT use which of the following procedures to identity events:

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

Answer: C

NEW QUESTION 438
- (Exam Topic 4)
John is using Management HA. Which Smartcenter should be connected to for making changes?

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

Answer: B

NEW QUESTION 439
- (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 444
- (Exam Topic 4)
Which method below is NOT one of the ways to communicate using the Management API's?

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

Answer: D

NEW QUESTION 448
- (Exam Topic 4)
Please choose correct command syntax to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

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

Answer: D

NEW QUESTION 450
- (Exam Topic 4)
What are the steps to configure the HTTPS Inspection Policy?

A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: C

NEW QUESTION 452
- (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 453
- (Exam Topic 4)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 457
- (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 462
- (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 465

- (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 467
- (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 470
- (Exam Topic 4)
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don’t have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

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

Answer: C

NEW QUESTION 472
- (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 473
- (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 476
- (Exam Topic 4)
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

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

Answer: D

NEW QUESTION 479
- (Exam Topic 4)
When an encrypted packet is decrypted, where does this happen?

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

Answer: A

NEW QUESTION 480
- (Exam Topic 4)
Under which file is the proxy arp configuration stored?

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

Answer: D

NEW QUESTION 483
- (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 484
- (Exam Topic 4)
Which repositories are installed on the Security Management Server by SmartUpdate?

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

Answer: D

NEW QUESTION 487
- (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 491
- (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 494
- (Exam Topic 4)
Which of the following is NOT a tracking option?

A. Partial log
B. Log
C. Network log
D. Full log

Answer: A

NEW QUESTION 495
- (Exam Topic 4)
Fill in the blanks. In _____ NAT, the _____ is translated.

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

Answer:

B

NEW QUESTION 500
- (Exam Topic 4)
In the Check Point Security Management Architecture, which component(s) can store logs?

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

Answer: B

NEW QUESTION 505
- (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 508
- (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 510
- (Exam Topic 4)
Fill in the blank: An LDAP server holds one or more _____.

A. Server Units
B. Administrator Units
C. Account Units
D. Account Server

Answer: C

NEW QUESTION 515
- (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 517
- (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 521
- (Exam Topic 4)
Phase 1 of the two-phase negotiation process conducted by IKE operates in a_____ mode.

A. Main
B. Authentication
C. Quick
D. High Alert

Answer: A

NEW QUESTION 522
- (Exam Topic 4)
You want to verify if there are unsaved changes in GAiA that will be lost with a reboot. What command can be used?

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

Answer: D

NEW QUESTION 525
- (Exam Topic 4)
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

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

Answer: A

NEW QUESTION 529
- (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 531
- (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 536
- (Exam Topic 4)
What command would show the API server status?

A. cpm status
B. api restart
C. api status
D. show api status

Answer: D

NEW QUESTION 539
- (Exam Topic 4)
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

A. Format; corporate
B. Local; formal
C. Local; central
D. Central; local

Answer: D

NEW QUESTION 540

- (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 542
- (Exam Topic 4)
How Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VP
B. Capsule Workspace provides a Desktop with usable applications
C. Capsule Workspace can provide access to any application
D. Capsule Connect provides Business data isolation
E. Capsule Connect does not require an installed application at client

Answer: A

NEW QUESTION 544
.....

Relate Links

100% Pass Your 156-215.80 Exam with Exambible 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/