156-215.80 Dumps

Check Point Certified Security Administrator

https://www.certleader.com/156-215.80-dumps.html

NEW QUESTION 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
Which of the following are types of VPN communicates?

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

Answer: D

NEW QUESTION 3
Which utility allows you to configure the DHCP service on GAIA from the command line?

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

Answer: C

Explanation: Sysconfig Configuration Options

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

NEW QUESTION 4
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 5
Which of the following technologies extracts detailed information from packets and stores that information in state tables?

A. INSPECT Engine
B. Stateful Inspection
C. Packet Filtering

D. Application Layer Firewall

Answer: B

NEW QUESTION 6
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:
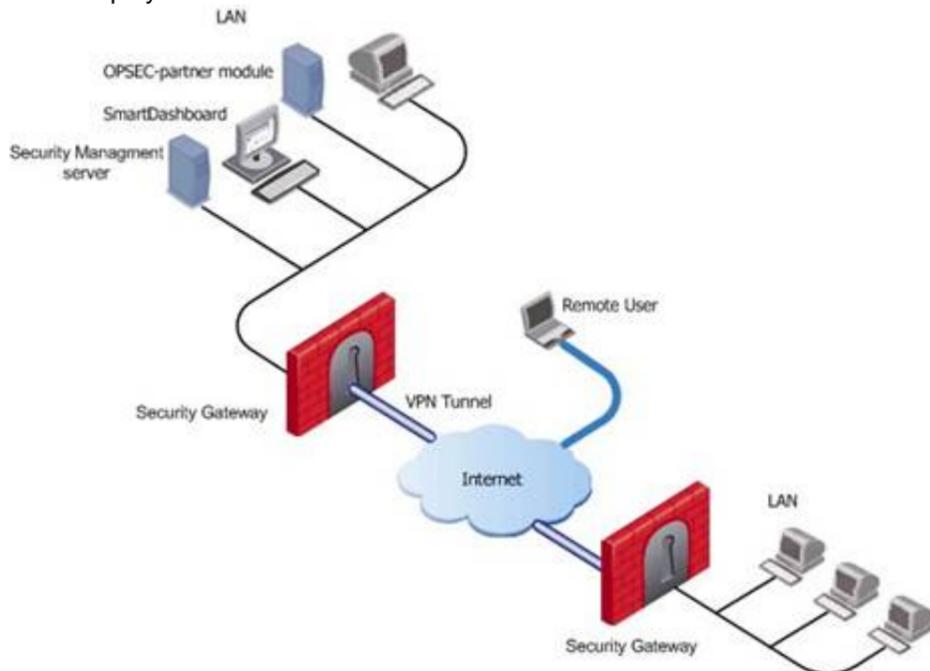
Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.
You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.
The Security Management server is 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 7
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 8
Which of the following is NOT a SecureXL traffic flow?

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

Answer: C

Explanation: SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:
Slow path - Packets and connections that are inspected by the Firewall and are not processed by SecureXL. Accelerated path - Packets and connections that are offloaded to SecureXL and are not processed by the
Firewall.
Medium path - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

NEW QUESTION 9
By default, which port does the WebUI listen on?

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

Answer: C

Explanation: To configure Security Management Server on Gaia:
Open a browser to the WebUI: https:<//Gaia management IP address>

NEW QUESTION 10
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

Answer: D

Explanation: There are different deployment scenarios for Check Point software products.
Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

NEW QUESTION 10
While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

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

Answer: B

Explanation: To enable Identity Awareness:
Log in to SmartDashboard.
From the Network Objects tree, expand the Check Poinbtranch.
Double-click the Security Gateway on which to enable Identity Awareness.
In the Software Blades section, select Identity Awarenesosn the Network Security tab. The Identity Awareness Configuration wizard opens.
Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.
AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers.
Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.
Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).
See Choosing Identity Sources.
Note - When you enable Browser-Based Authentication on a Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.
Click Next.
The Integration With Active Directory window opens.
When SmartDashboard is part of the domain, SmartDashboard suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with alolf the domain controllers in the organization's Active Directory.

NEW QUESTION 12
Which default user has full read/write access?

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

Answer: C

NEW QUESTION 15
Which of the following is TRUE regarding Gaia command line?

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

Answer: D

NEW QUESTION 16
Two administrators Dave and Jon both manage R80 Management as administrators for ABC Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it his in his SmartConsole view?
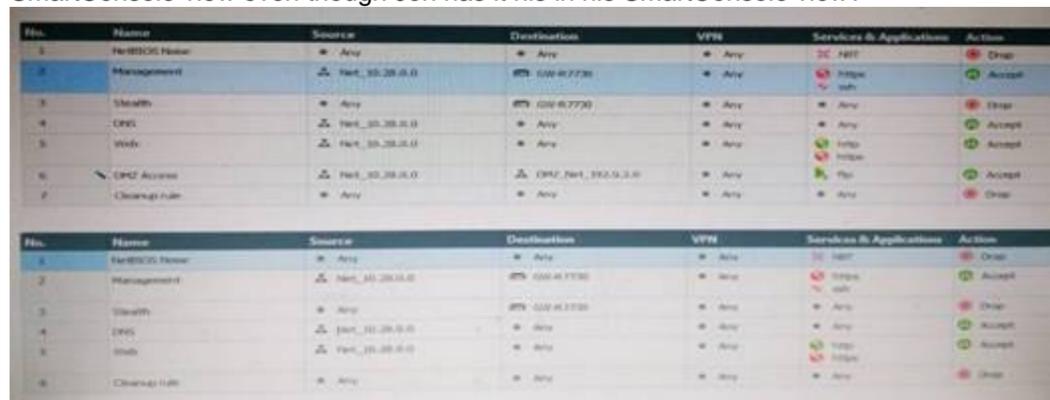
A. Jon is currently editing rule no.6 but has Published part of his changes.
B. Dave is currently editing rule no.6 and has marked this rule for deletion.
C. Dave is currently editing rule no.6 and has deleted it from his Rule Base.
D. Jon is currently editing rule no.6 but has not yet Published his changes.

Answer: D

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

NEW QUESTION 19
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 20
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 25
Fill in the blank: To build an effective Security Policy, use a _____ and _____ rule.

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

Answer: A

NEW QUESTION 28
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 29
DLP and Geo Policy are examples of what type of Policy?

A. Standard Policies
B. Shared Policies
C. Inspection Policies
D. Unified Policies

Answer: B

Explanation: The Shared policies are installed with the Access Control Policy.

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

NEW QUESTION 32
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

A. Security questions
B. Check Point password
C. SecurID

D. RADIUS

Answer: A

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

NEW QUESTION 33
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____ .

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

Answer: B

Explanation: To enable Identity Awareness:
 Log in to SmartDashboard.
 From the Network Objects tree, expand the Check Point branch.
 Double-click the Security Gateway on which to enable Identity Awareness.
 In the Software Blades section, select Identity Awareness on the Network Security tab.
The Identity Awareness
Configuration wizard opens.
 Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.
 AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers
 Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

NEW QUESTION 38
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 39
What will be the effect of running the following command on the Security Management Server?
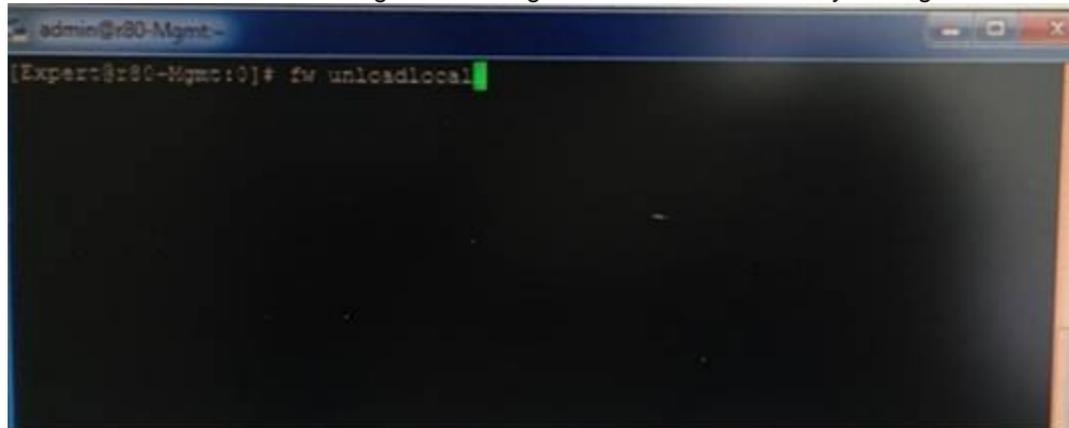
A. Remove the installed Security Policy.
B. Remove the local ACL lists.
C. No effect.
D. Reset SIC on all gateways.

Answer: A

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

NEW QUESTION 41
View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.
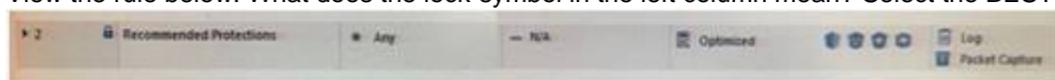
A. The current administrator has read-only permissions to Threat Prevention Policy.
B. Another user has locked the rule for editing.
C. Configuration lock is presen
D. Click the lock symbol to gain read-write access.
E. The current administrator is logged in as read-only because someone else is editing 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 42
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 45
Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
B. One machine
C. Two machines
D. Three machines

Answer: C

Explanation: One for Security Management Server and the other one for the Security Gateway.

NEW QUESTION 49
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:
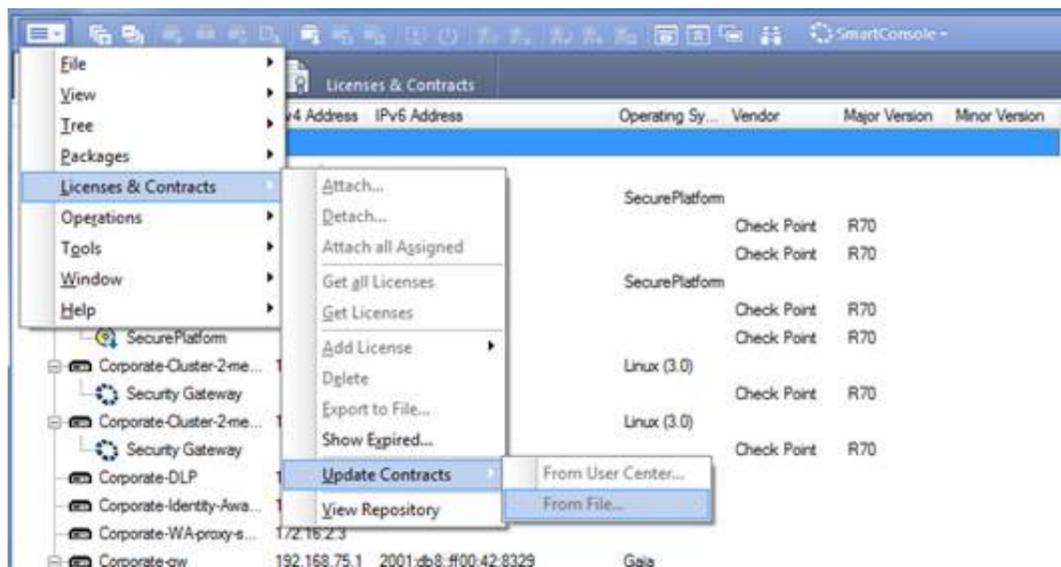
Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.

NEW QUESTION 54
Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

A. /var/log/Cpbackup/backups/backup/backup_fw.tgs
B. /var/log/Cpbackup/backups/backup/backup_fw.tar
C. /var/log/Cpbackup/backups/backups/backup_fw.tar
D. /var/log/Cpbackup/backups/backup_fw.tgz

Answer: D

Explanation: Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration. The configuration is saved to a .tgz file in the following directory:
Gaia OS Version Hardware
Local Directory R75.40 - R77.20
Check Point appliances
/var/log/CPbackup/backups/ Open Server
/var/CPbackup/backups/ R77.30
Check Point appliances
/var/log/CPbackup/backups/ Open Server

NEW QUESTION 59
Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

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

Answer: C

NEW QUESTION 60
What are the three authentication methods for SIC?

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

Answer: B

Explanation: Secure Internal Communication (SIC)
Secure Internal Communication (SIC) lets Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components. SIC is required to install polices on gateways and to send logs between gateways and management servers.
These security measures make sure of the safety of SIC:
 Certificates for authentication
 Standards-based SSL for the creation of the secure channel
 3DES for encryption
References:

NEW QUESTION 61
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 62
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 65
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 66
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 70
Which Check Point feature enables application scanning and the detection?

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

Answer: B

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

NEW QUESTION 75
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 79
Which of the following is NOT a license activation method?

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

Answer: A

NEW QUESTION 82
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 86
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 87
If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

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

Answer: A

Explanation: To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.
To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.
When you select Install Policy, you are prompted to publish all unpublished changes. You cannot install a policy if the included changes are not published.

NEW QUESTION 91
Which options are given on features, when editing a Role on Gaia Platform?

A. Read/Write, Read Only
B. Read/Write, Read only, None
C. Read/Write, None
D. Read Only, None

Answer: B

Explanation: Roles
Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (readonly) access to other features, and no access to other features.
You can also specify which access mechanisms (WebUI or the CLI) are available to the user.
Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.
Gaia includes these predefined roles:
You cannot delete or change the predefined roles.
Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

NEW QUESTION 92
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 93
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 97
Packages and licenses are loaded from all of these sources EXCEPT

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

Answer: B

Explanation: the Download Center web site (packages)
the Check Point DVD (packages)
the User Center (licenses)
by importing a file (packages and licenses)
by running the cplic command line
Packages and licenses are loaded into these repositories from several sources: References:

NEW QUESTION 102
On the following graphic, you will find layers of policies.
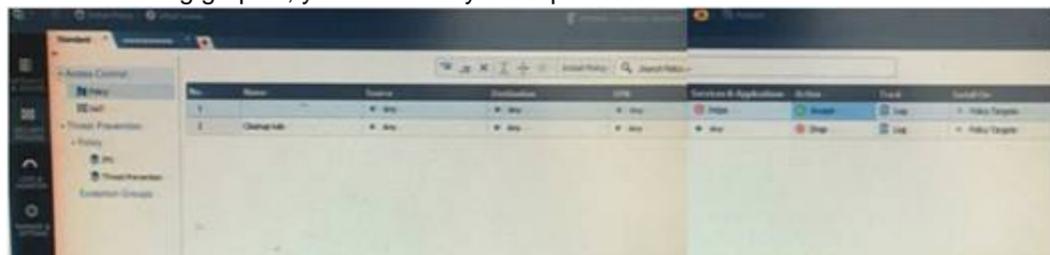
What is a precedence of traffic inspection for the defined polices?

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 103
Fill in the blank: The tool _____ generates a R80 Security Gateway configuration report.

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

Answer: C

Explanation: CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).
The CPinfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPinfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.
When contacting Check Point Support, collect the cpinfo files from the Security Management server and Security Gateways involved in your case.

NEW QUESTION 108
Fill in the blank: The _____ collects logs and sends them to the _____.

A. Log server; security management server
B. Log server; Security Gateway
C. Security management server; Security Gateway
D. Security Gateways; log server

Answer: D

NEW QUESTION 112
Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when _____.

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

Answer: A

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

NEW QUESTION 116
When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

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

Answer: C

NEW QUESTION 118
What are the three conflict resolution rules in the Threat Prevention Policy Layers?

A. Conflict on action, conflict on exception, and conflict on settings

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

Answer: C

NEW QUESTION 120
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 124
Where can you trigger a failover of the cluster members?
Log in to Security Gateway CLI and run command clusterXL_admin down.
In SmartView Monitor right-click the Security Gateway member and select Cluster member stop. Log into Security Gateway CLI and run command cphaprob down.

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

Answer: C

Explanation: How to Initiate Failover

Method	To Stop ClusterXL	To Start ClusterXL
Run: o cphaprob -d faildevice -t 0 -s ok register o cphaprob -d faildevice -s problem report and: o cphaprob -d faildevice -s ok report o cphaprob -d faildevice unregister	Effect: o Disables ClusterXL o Does not disable synchronization	Effect: o Enables ClusterXL o Does not initiate full synchronization
Recommended method: Run: o clusterXL_admin down o clusterXL_admin up	o Disables ClusterXL o Does not disable synchronization	o Enables ClusterXL o Does not initiate full synchronization
In SmartView Monitor: 1. Click the Cluster object. 2. Select one of the member gateway branches. 3. Right click the cluster member. 4. Select **Down**.	o Disables ClusterXL o Disables synchronization	o Enables ClusterXL o Does not initiate full synchronization

NEW QUESTION 129
Fill in the blank: Each cluster has _____ interfaces.

A. Five
B. Two
C. Three
D. Four

Answer: C

Explanation: Each cluster member has three interfaces: one external interface, one internal interface, and one for synchronization. Cluster member interfaces facing in each direction are connected via a switch, router, or VLAN switch.

NEW QUESTION 132
What are the two high availability modes?

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

Answer: D

Explanation: ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.
Load Sharing Multicast Mode
Load Sharing Unicast Mode
New High Availability Mode
High Availability Legacy Mode

NEW QUESTION 133
To optimize Rule Base efficiency, the most hit rules should be where?

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

Answer: C

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

NEW QUESTION 138
Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

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

Answer: C

Explanation: Suspicious Activity Rules Solution
Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).
The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation

NEW QUESTION 140
You are unable to login to SmartDashboard. You log into the management server and run #cpwd_admin list with the following output:

What reason could possibly BEST explain why you are unable to connect to SmartDashboard?

A. CDP is down
B. SVR is down
C. FWM is down
D. CPSM is down

Answer: C

Explanation: The correct answer would be FWM (is the process making available communication between SmartConsole applications and Security Management Server.). STATE is T (Terminate = Down)
Symptoms
 SmartDashboard fails to connect to the Security Management server.
 Verify if the FWM process is running. To do this, run the command:
[Expert@HostName:0]# ps -aux | grep fwm
 If the FWM process is not running, then try force-starting the process with the following command: [Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm" [Expert@HostName:0]# ps -aux | grep fwm
[Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"

NEW QUESTION 144
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 148
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 150
Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?

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

Answer: B

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

NEW QUESTION 151
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 156
Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.
Where can the administrator check for more information on these errors?
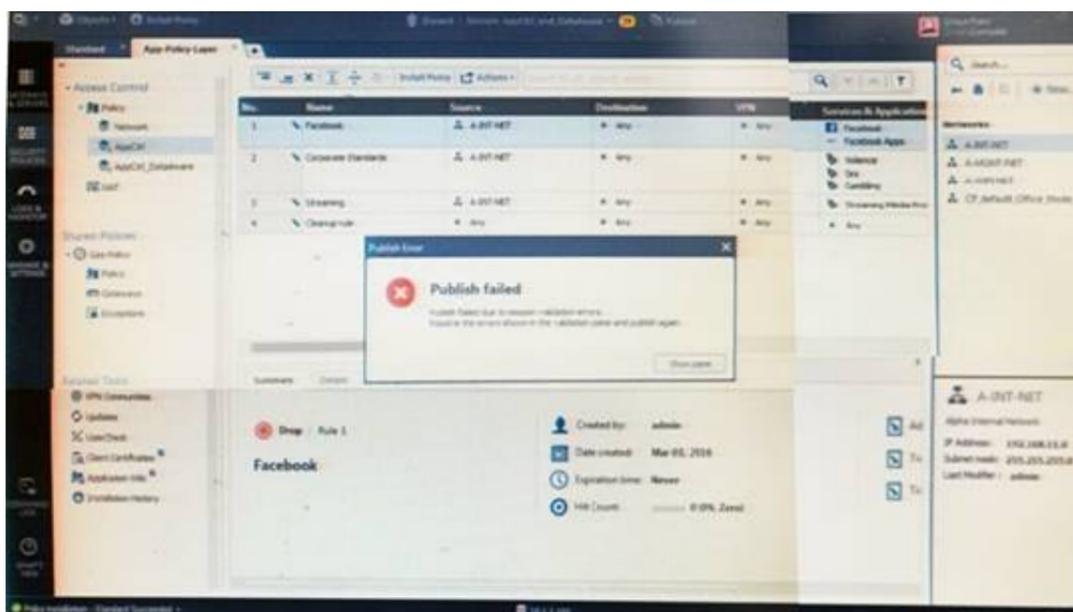
A. The Log and Monitor section in SmartConsole
B. The Validations section in SmartConsole
C. The Objects section in SmartConsole
D. The Policies section in SmartConsole

Answer: B

Explanation: Validation Errors
The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.
To publish, you must fix the errors.

NEW QUESTION 159
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 163
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'?
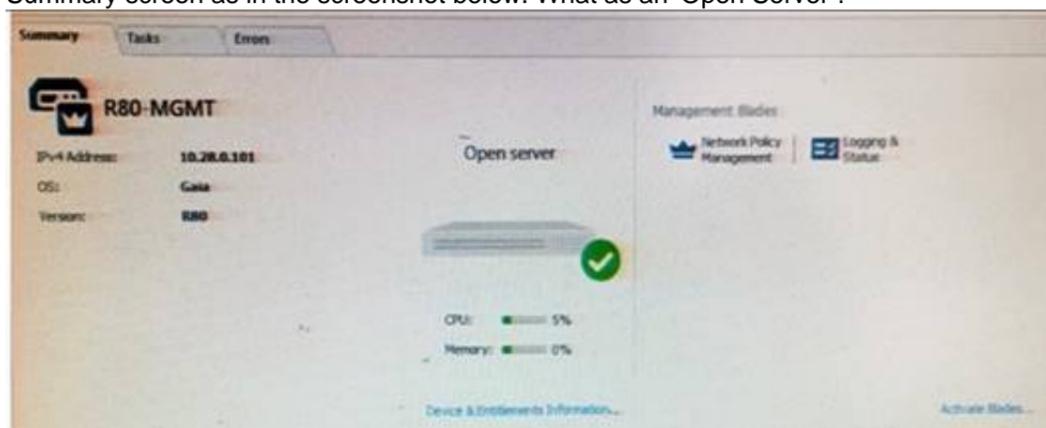
A. Check Point software deployed on a non-Check Point appliance.
B. The Open Server Consortium approved Server Hardware used for the purpose of Security and Availability.
C. A check Point Management Server deployed using the Open Systems Interconnection (OSI) Server andSecurity deployment model.
D. A check Point Management Server software using the Open SSL.

Answer: A

Explanation:

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

Topic 2, Exam Pool B

NEW QUESTION 166
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 167
You want to reset SIC between smberlin and sgosaka.
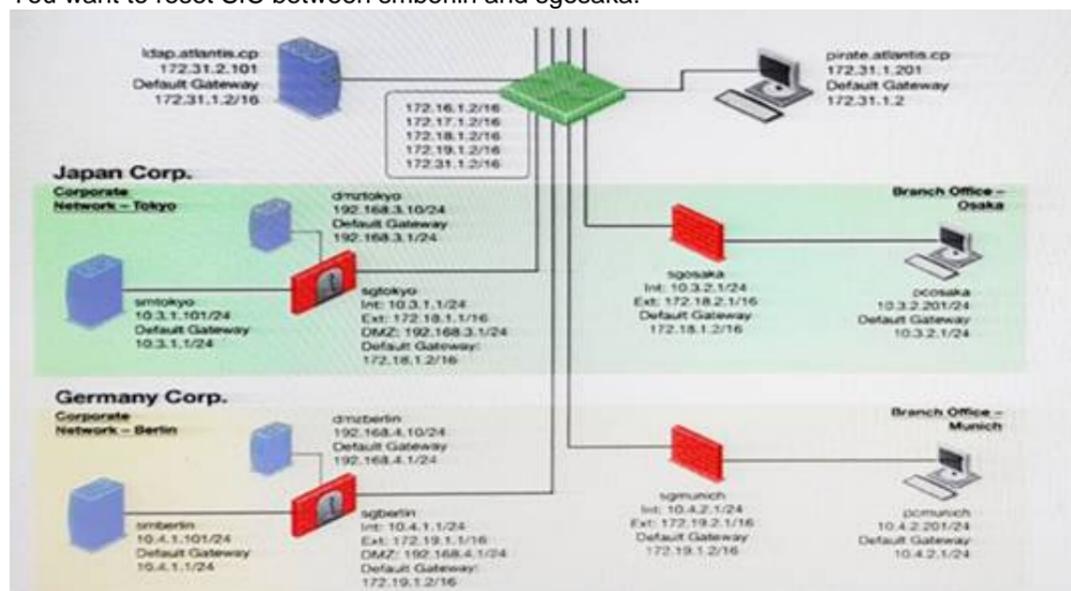
In SmartDashboard, you choose sgosaka, Communication, Reset. On sgosaka, you start cpconfig, choose Secure Internal Communication and enter the new SIC Activation Key. The screen reads The SIC was successfully initialized and jumps back to the menu. When trying to establish a connection, instead of a 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 169
To install a brand new Check Point Cluster, the MegaCorp IT department bought 1 Smart-1 and 2 Security Gateway Appliances to run a cluster. Which type of cluster is it?

A. Full HA Cluster
B. High Availability
C. Standalone
D. Distributed

Answer: B

NEW QUESTION 172
In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

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

Answer: A

NEW QUESTION 177
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 182
What are the three tabs available in SmartView Tracker?

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

Answer: C

NEW QUESTION 183
Can a Check Point gateway translate both source IP address and destination IP address in a given packet?

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

Answer: A

NEW QUESTION 185
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 187
Why would an administrator see the message below?
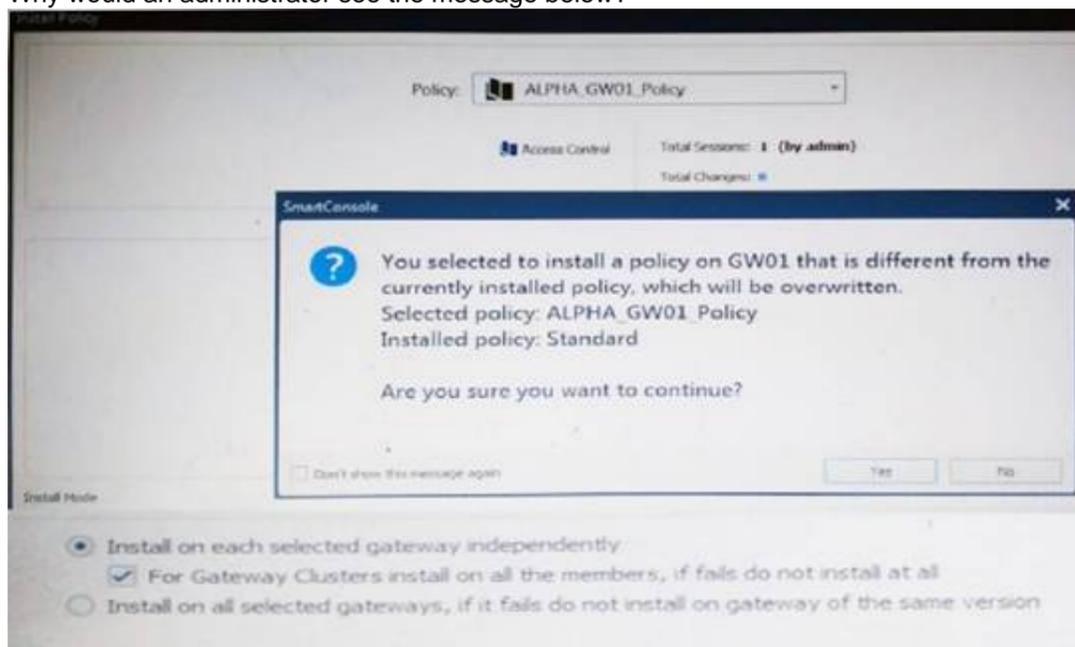
A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
C. A new Policy Package created on the Gateway is going to be installed 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 192
What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.
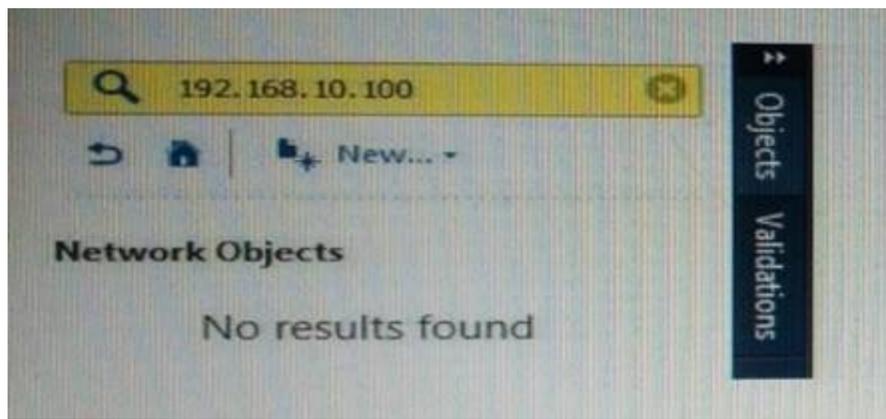
A. Search detailed is missing the subnet mask.
B. There is no object on the database with that name or that IP address.
C. There is no object on the database with that IP address.
D. Object does not have a NAT IP address.

Answer: B

NEW QUESTION 195
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 196
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 201
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 206
Fill in the blank: The _____ software blade enables Application Security policies to allow, block, or limit website access based on user, group, and machine identities.

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

Answer: A

NEW QUESTION 211
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 212
Choose what BEST describes a Session.

A. Starts when an Administrator publishes all the changes made on SmartConsole.
B. Starts when an Administrator logs in to the Security Management Server through SmartConsole and ends when it is published.
C. Sessions ends when policy is pushed to the Security Gateway.
D. Sessions locks the policy package for editing.

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 213
Fill in the blanks: A Check Point software license consists of a _____ and _____.

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

Answer: B

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

NEW QUESTION 216
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 218
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 220
Which directory holds the SmartLog index files by default?

A. $SMARTLOGDIR/data
B. $SMARTLOG/dir
C. $FWDIR/smartlog
D. $FWDIR/log

Answer: A

NEW QUESTION 222
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 224
Study the Rule base and Client Authentication Action properties screen.
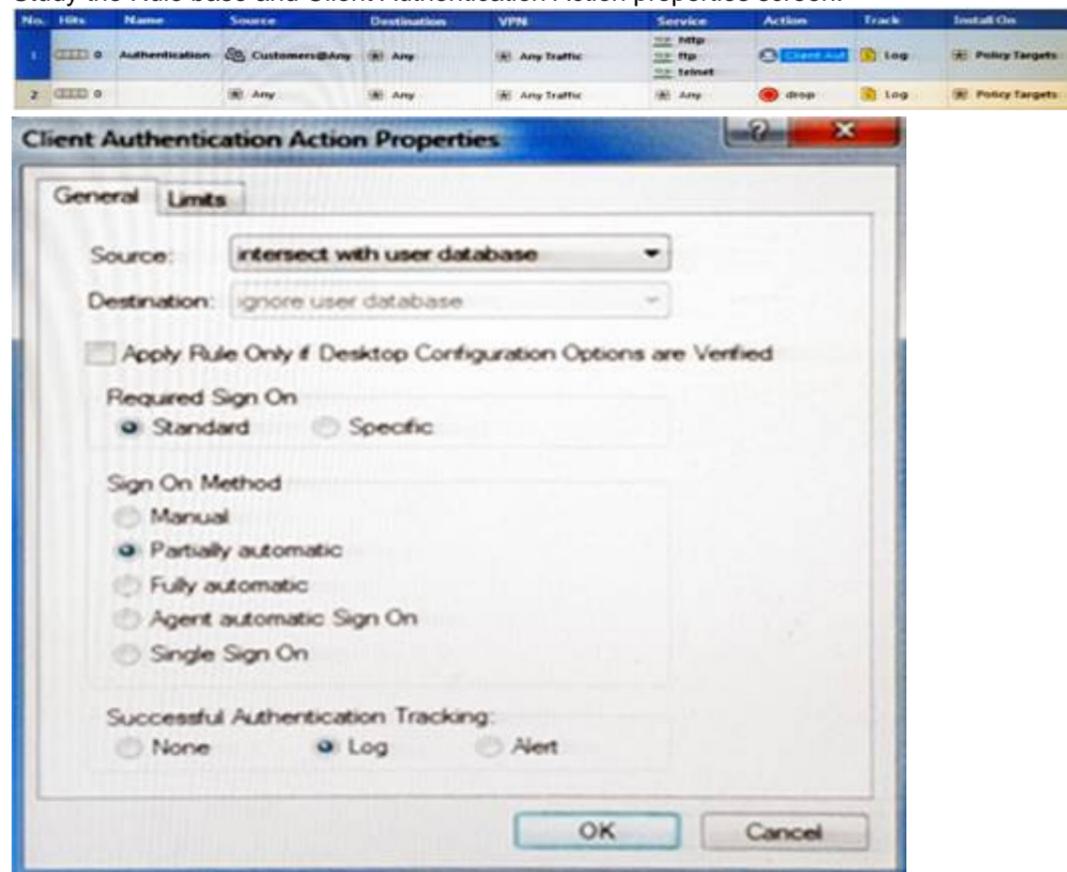
After being authenticated by the Security Gateways, a user starts a HTTP connection to a Web site. What happens when the user tries to FTP to another site using the command line? The:

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

Answer: C

NEW QUESTION 226
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 227
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 232
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 234
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 236
Choose what BEST describes users on Gaia Platform.

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

Answer: B

Explanation: These users are created by default and cannot be deleted:
 admin — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user
has a User ID of 0, and therefore has all of the privileges of a root user.
 monitor — Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.

NEW QUESTION 237
Administrator wishes to update IPS from SmartConsole by clicking on the option "update now" under the IPS tab. Which device requires internet access for the update to work?

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

Answer: B

Explanation: Updating IPS Manually
You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website. You can only manually update IPS if a proxy is defined in Internet Explorer settings.
To obtain updates of all the latest protections from the IPS website:
 Configure the settings for the proxy server in Internet Explorer.
 In Microsoft Internet Explorer, open Tools > Internet Options > Connections tab > LAN Settings.
The LAN Settings window opens.
 Select Use a proxy server for your LAN.
 Configure the IP address and port number for the proxy server.
 Click OK.
The settings for the Internet Explorer proxy server are configured.
 In the IPS tab, select Download Updates
and clickUpdate Now.

NEW QUESTION 238
What is the default shell of Gaia CLI?

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

Answer: B

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

NEW QUESTION 240
Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

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

Answer: C

NEW QUESTION 243
Which SmartConsole component can Administrators use to track changes to the Rule Base?

A. WebUI
B. SmartView Tracker
C. SmartView Monitor
D. SmartReporter

Answer: B

NEW QUESTION 244
Look at the screenshot below. What CLISH command provides this output?

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

Answer: D

NEW QUESTION 248
Anti-Spoofing is typically set up on which object type?

A. Security Gateway
B. Host
C. Security Management object
D. Network

Answer: A

NEW QUESTION 251
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 254
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 256
What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

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

Answer: D

NEW QUESTION 260
The IT Management team is interested in the new features of the Check Point R80 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80 because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

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

Answer: A

NEW QUESTION 265
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 269
The most important part of a site-to-site VPN deployment is the _____.

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

Answer: C

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

NEW QUESTION 274
Look at the following screenshot and select the BEST answer.
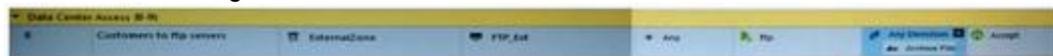
A. Clients external to the Security Gateway can download archive files from FTP_Ext server using FTP.
B. Internal clients can upload and download any-files to FTP_Ext-server using FTP.
C. Internal clients can upload and download archive-files to FTP_Ext server using FTP.
D. Clients external to the Security Gateway can upload any files to the FTP_Ext-server using FTP.

Answer: A

NEW QUESTION 278
Which information is included in the "Full Log" tracking option, but is not included in the "Log" tracking option?

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

Answer: D

Explanation: Network Log - Generates a log with only basic Firewall information: Source, Destination, Source Port, Destination Port, and Protocol.
Log - Equivalent to the Network Log option, but also includes the application name (for example, Dropbox), and application information (for example, the URL of the Website). This is the default Tracking option.
Full Log - Equivalent to the log option, but also records data for each URL request made.
If suppression is not selected, it generates a complete log (as defined in pre-R80 management).
If suppression is selected, it generates an extended log(as defined in pre-R80 management).
None - Do not generate a log.

NEW QUESTION 279
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 284
Which authentication scheme requires a user to possess a token?

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

Answer: B

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

NEW QUESTION 288
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 289
You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the
most likely cause?

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

Answer: C

NEW QUESTION 291
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 295
Which of the following licenses are considered temporary?

A. Perpetual and Trial
B. Plug-and-play and Evaluation
C. Subscription and Perpetual
D. Evaluation and Subscription

Answer: B

Explanation: Should be Trial or Evaluation, even Plug-and-play (all are synonyms). Answer B is the best choice.

NEW QUESTION 298
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 302
On the following picture an administrator configures Identity Awareness:
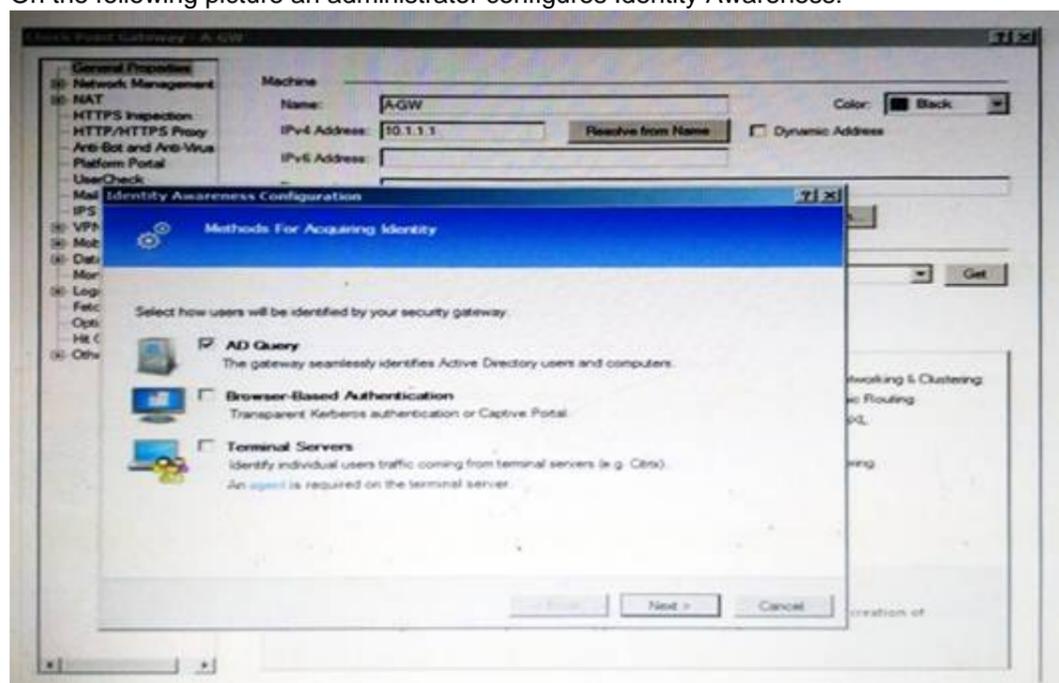
After clicking "Next" the above configuration is supported by:

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 307
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 310
Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

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

Answer: C

NEW QUESTION 315
Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

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

Answer: A

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

NEW QUESTION 317
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 321
Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?

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

Answer: A

Explanation: Did you know: mgmt_cli can accept csv files as inputs using the --batch option.
The first row should contain the argument names and the rows below it should hold the values for these parameters.
So an equivalent solution to the powershell script could look like this:
data.csv:

name	ipv4-address	color
host1	192.168.35.1	black
host2	192.168.35.2	red
host3	192.168.35.3	blue

mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server>
This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

NEW QUESTION 323
The organization's security manager wishes to back up just the Gaia operating system parameters. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries?

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

Answer: B

Explanation: 3. System Backup (and System Restore)
System Backup can be used to backup current system configuration. A backup creates a compressed file that contains the Check Point configuration including the networking and operating system parameters, such as routing and interface configuration etc., but unlike a snapshot, it does not include the operating system, product binaries, and hotfixes.

Topic 3, Exam Pool C

NEW QUESTION 326
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 327
In what way are SSL VPN and IPSec VPN different?

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

Answer: D

NEW QUESTION 330
The Firewall kernel is replicated multiple times, therefore:

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

Answer: D

NEW QUESTION 333
Where do you verify that UserDirectory is enabled?

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

Answer: D

NEW QUESTION 338
According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

A. Interoperable Device
B. Network Node

C. Externally managed gateway
D. Gateway

Answer: A

NEW QUESTION 340
The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them?

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

Answer: D

NEW QUESTION 344
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 348
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 353
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 358
What is also referred to as Dynamic NAT?

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

Answer: D

NEW QUESTION 362
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 367
Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

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

Answer: C

NEW QUESTION 372
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 376
Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except:

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

Answer: A

NEW QUESTION 377
To fully enable Dynamic Dispatcher on a Security Gateway:

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

Answer: A

NEW QUESTION 382
What is the difference between an event and a log?

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

Answer: B

NEW QUESTION 386
Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

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

Answer: B

NEW QUESTION 388
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 390
How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

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

Answer: C

NEW QUESTION 392
A digital signature:

A. Guarantees the authenticity and integrity of a message.
B. Automatically exchanges shared keys.
C. Decrypts data to its original form.
D. Provides a secure key exchange mechanism over the Internet.

Answer: A

NEW QUESTION 393
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 398
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 402
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 403
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 404
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 406
The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the following should you remember?

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

Answer: B

NEW QUESTION 409
What is Consolidation Policy?

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

Answer: B

NEW QUESTION 414
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 418
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 420
Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

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

Answer: C

NEW QUESTION 423
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via
e-m ail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and
only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?

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

Answer: D

NEW QUESTION 428
What is the Manual Client Authentication TELNET port?

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

Answer: D

NEW QUESTION 430
Where does the security administrator activate Identity Awareness within SmartDashboard?

A. Gateway Object > General Properties
B. Security Management Server > Identity Awareness
C. Policy > Global Properties > Identity Awareness
D. LDAP Server Object > General Properties

Answer: A

NEW QUESTION 431
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 433
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 437
While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?
1) Select Active Mode tab in SmartView Tracker.
2) Select Tools > Block Intruder.
3) Select Log Viewing tab in SmartView Tracker.
4) Set Blocking Timeout value to 60 minutes.
5) Highlight connection that should be blocked.

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

Answer: C

NEW QUESTION 438
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 439
Which set of objects have an Authentication tab?

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

Answer: A

NEW QUESTION 442
Which one of the following is true about Threat Extraction?

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

Answer: B

NEW QUESTION 447
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 448
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 453
Which of the following is NOT an attribute of packer acceleration?

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

Answer: D

NEW QUESTION 458
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 462
How do you configure an alert in SmartView Monitor?

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

Answer: B

NEW QUESTION 463
According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added? A(n):

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

Answer: C

NEW QUESTION 464
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 466
What is the appropriate default Gaia Portal address?

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

Answer: D

NEW QUESTION 470
When launching SmartDashboard, what information is required to log into R77?

A. User Name, Management Server IP, certificate fingerprint file
B. User Name, Password, Management Server IP

C. Password, Management Server IP
D. Password, Management Server IP, LDAP Server IP

Answer: B

NEW QUESTION 473
Which component functions as the Internal Certificate Authority for R77?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLSM

Answer: B

NEW QUESTION 477
Which R77 GUI would you use to see number of packets accepted since the last policy install?

A. SmartView Monitor
B. SmartView Tracker
C. SmartDashboard
D. SmartView Status

Answer: A

NEW QUESTION 482
Which tool CANNOT be launched from SmartUpdate R77?

A. IP Appliance Voyager
B. snapshot
C. GAiA WebUI
D. cpinfo

Answer: B

NEW QUESTION 486
When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

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

Answer: C

NEW QUESTION 487
When defining QoS global properties, which option below is not valid?

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

Answer: C

NEW QUESTION 488
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 489
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 492
What are types of Check Point APIs available currently as part of R80.10 code?

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

Answer: B

NEW QUESTION 494
If the first packet of an UDP session is rejected by a security policy, what does the firewall send to the client?

A. Nothing
B. TCP FIN
C. TCP RST
D. ICMP unreachable

Answer: A

NEW QUESTION 496
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 498
Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

A. Source Address
B. Destination Address
C. TCP Acknowledgment Number
D. Source Port

Answer: C

NEW QUESTION 499
What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?

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

Answer: B

NEW QUESTION 504
Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made:

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

Answer: A

NEW QUESTION 507
How are the backups stored in Chock Point appliances?

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

Answer: D

NEW QUESTION 511
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 514
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 519
What is the BEST method to deploy identity Awareness for roaming users?

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

Answer: A

NEW QUESTION 521
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 522
Which of the following is NOT a component of Check Point Capsule?

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

Answer: C

NEW QUESTION 524
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

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

Answer: B

NEW QUESTION 525
From SecureXL perspective, what are the tree paths of traffic flow:

A. Initial Path; Medium Path; Accelerated Path
B. Layer Path; Blade Path; Rule Path
C. Firewall Path; Accept Path; Drop Path
D. Firewall Path; Accelerated Path; Medium Path

Answer: D

NEW QUESTION 529
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 532
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 536
Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

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

Answer: C

NEW QUESTION 539
Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays _____ for the given VPN tunnel.

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

Answer: A

NEW QUESTION 544
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 546
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 547
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 552
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 553
What Identity Agent allows packet tagging and computer authentication?

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

Answer: B

NEW QUESTION 557
Which is a suitable command to check whether Drop Templates are activated or not?

A. fw ctl get int activate_drop_templates
B. fwaccel stat
C. fwaccel stats
D. fw ctl templates –d

Answer: B

NEW QUESTION 562
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 565
What is the Transport layer of the TCP/IP model responsible for?

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

Answer: B

NEW QUESTION 568
Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Answer: B

NEW QUESTION 571
Using ClusterXL, what statement is true about the Sticky Decision Function?

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

Answer: A

NEW QUESTION 572
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 573
What is the purpose of the Clean-up Rule?

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

Answer: A

NEW QUESTION 574
You can see the following graphic:
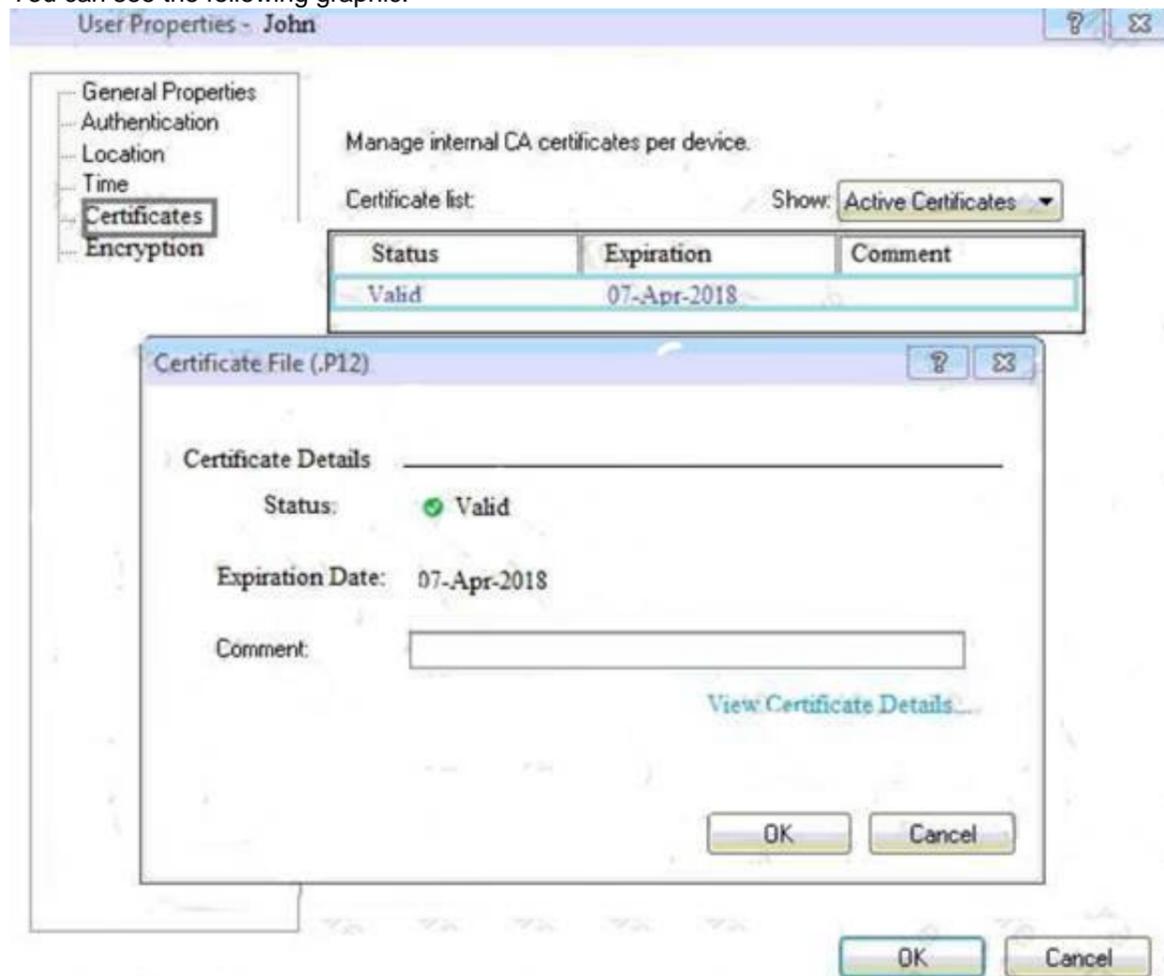
What is presented on it?

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

Answer: A

NEW QUESTION 575
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 580
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 582
What two ordered layers make up the Access Control Policy Layer?

A. URL Filtering and Network
B. Network and Threat Prevention
C. Application Control and URL Filtering
D. Network and Application Control

Answer: C

NEW QUESTION 583
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 587
......

Thank You for Trying Our Product

* 100% Pass or Money Back

   All our products come with a 90-day Money Back Guarantee.

* One year free update

   You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

   We currently serve more than 30,000,000 customers.

* Shop Securely

   All transactions are protected by VeriSign!

100% Pass Your 156-215.80 Exam with Our Prep Materials Via below:

https://www.certleader.com/156-215.80-dumps.html