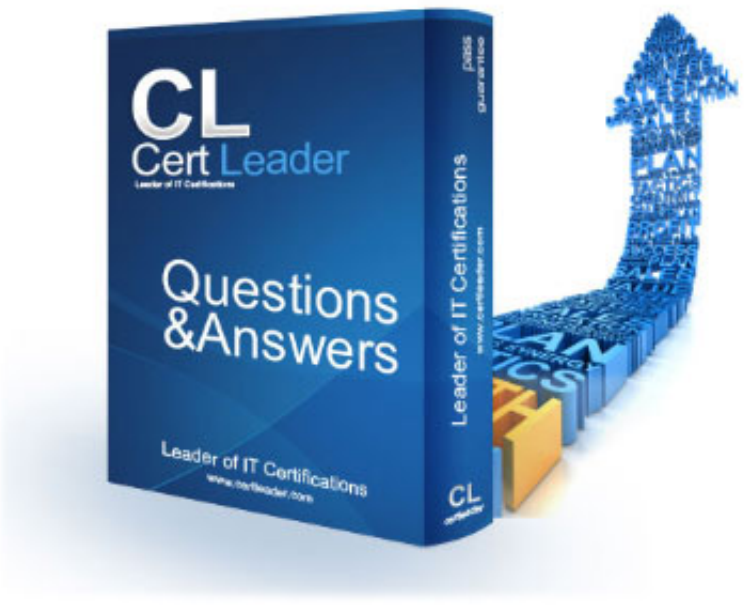
156-215.80 Dumps

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
What does the “unknown” SIC status shown on SmartConsole mean?

A. The SMS can contact the Security Gateway but cannot establish Secure Internal Communication.
B. SIC activation key requires a reset.
C. The SIC activation key is not known by any administrator.
D. There is no connection between the Security Gateway and SMS.

Answer: D

Explanation: The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is Unknown then there is no connection between the Gateway an the Security Management server. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

NEW QUESTION 5
You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

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

Answer: A

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

NEW QUESTION 6
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 7
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

Answer: D

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

NEW QUESTION 8
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 9
The Gaia operating system supports which routing protocols?

A. BGP, OSPF, RIP
B. BGP, OSPF, EIGRP, PIM, IGMP
C. BGP, OSPF, RIP, PIM, IGMP
D. BGP, OSPF, RIP, EIGRP

Answer: A

Explanation: The Advanced Routing Suite
The Advanced Routing Suite CLI is available as part of the Advanced Networking Software Blade.
For organizations looking to implement scalable, fault-tolerant, secure networks, the Advanced Networking blade enables them to run industry-standard dynamic routing protocols including BGP, OSPF, RIPv1, and RIPv2 on security gateways. OSPF, RIPv1, and RIPv2 enable dynamic routing over a single autonomous system—like a single department, company, or service provider—to avoid network failures. BGP provides dynamic routing support across more complex networks involving multiple autonomous systems—such as when a company uses two service providers or divides a network into multiple areas with different administrators responsible for the performance of each.

NEW QUESTION 10
Which default user has full read/write access?

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

Answer: C

NEW QUESTION 10
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)

Description	1. Add, change or delete role definitions. 2. Add or remove users to or from existing roles. 3. Add or remove access mechanism (WebUI or CLI) permissions for a specified user.

Syntax	`add rba role <Name> domain-type System`
	`readonly-features <List>`
	`readwrite-features <List>`
	
	`add rba user <User name> access-mechanisms [Web-UI | CLI]`
	`add rba user <User Name> roles <List>`
	
	`delete rba role <Name>`
	
	`delete rba role <Name>`
	`readonly-features <List>`
	`readwrite-features <L`
	
	`delete rba user <User Name> access-mechanisms [Web-UI | CLI]`
	`delete rba user <User Name> roles <List>`

NEW QUESTION 13
Fill in the blank: The R80 utility fw monitor is used to troubleshoot _____

A. User data base corruption
B. LDAP conflicts
C. Traffic issues
D. Phase two key negotiation

Answer: C

Explanation: Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark

NEW QUESTION 18
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 22
Vanessa is firewall administrator in her company; her company is using Check Point firewalls on central and remote locations, which are managed centrally by R80

Security Management Server. One central location has an installed R77.30 Gateway on Open server. Remote location is using Check Point UTM-1 570 series appliance with R71. Which encryption is used in Secure Internal Communication (SIC) between central management and firewall on each location?

A. On central firewall AES128 encryption is used for SIC, on Remote firewall 3DES encryption is used for SIC.
B. On both firewalls, the same encryption is used for SI
C. This is AES-GCM-256.
D. The Firewall Administrator can choose which encryption suite will be used by SIC.
E. On central firewall AES256 encryption is used for SIC, on Remote firewall AES128 encryption is used for SIC.

Answer: A

Explanation: Gateways above R71 use AES128 for SIC. If one of the gateways is R71 or below, the gateways use 3DES.

NEW QUESTION 23
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 26
ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house R80 Management to the other administrators in ABC Corp.

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

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

Answer: C

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

NEW QUESTION 29
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 34
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 37
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 41
Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

A. remove database lock
B. The database feature has one command lock database override.
C. override database lock
D. The database feature has two commands: lock database override and unlock databas
E. Both will work.

Answer: D

Explanation: Use the database feature to obtain the configuration lock. The database feature has two commands:
lock database [override].
unlock database
The commands do the same thing: obtain the configuration lock from another administrator.

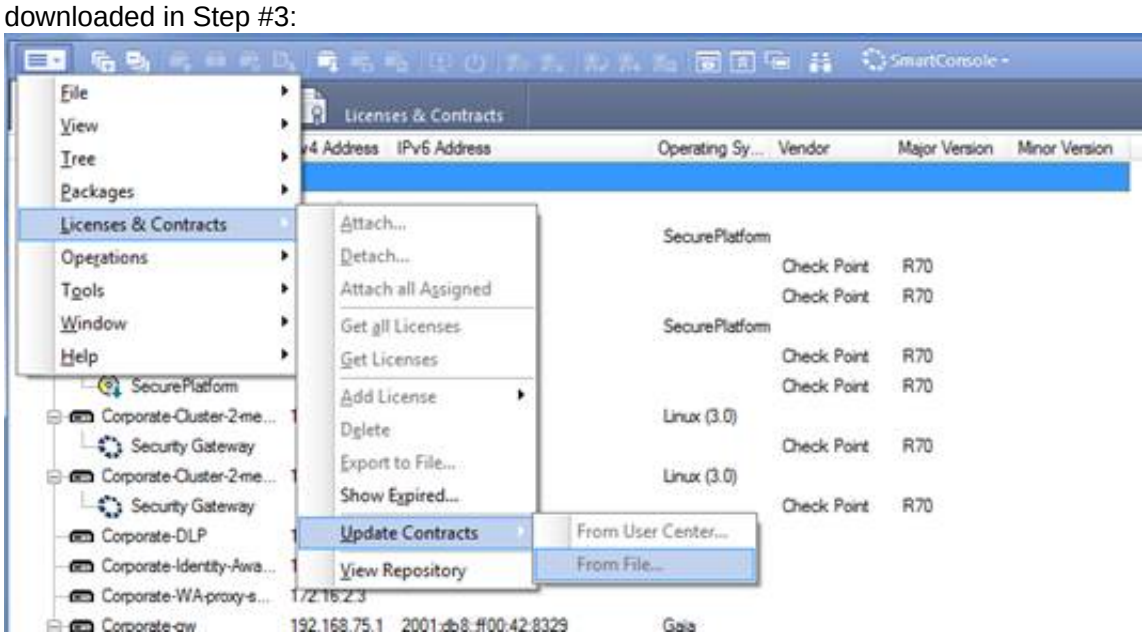
Description	Use the `lock database override` and `unlock database` commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	o `lock database override` o `unlock database`

NEW QUESTION 45
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 47
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

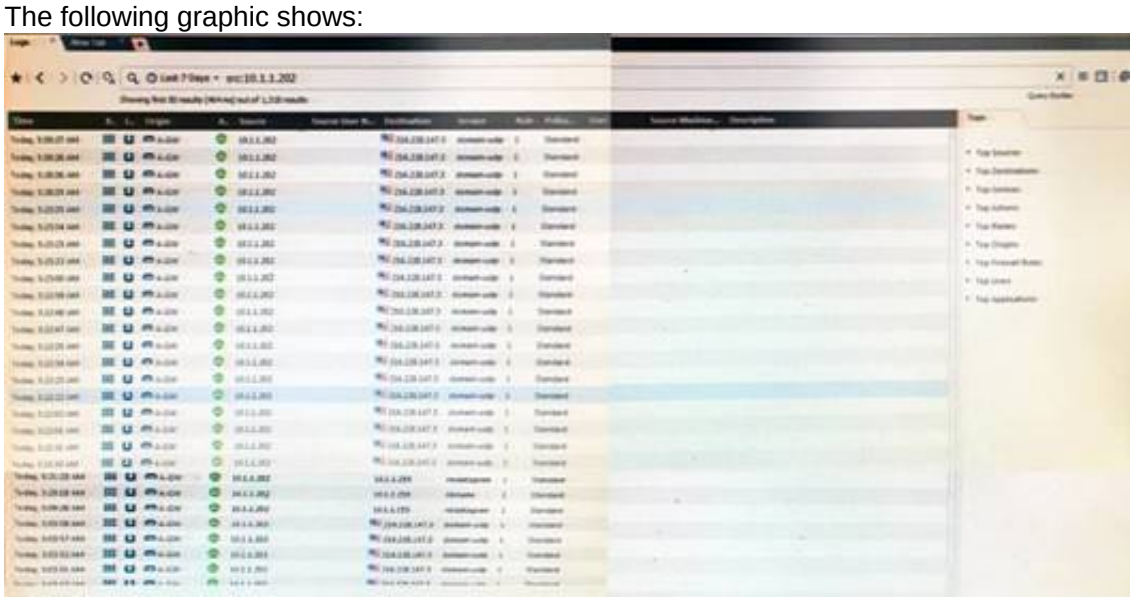
Answer: C

NEW QUESTION 52
Fill in the blank: The ____ is used to obtain identification and security information about network users.

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

Answer: A

NEW QUESTION 55
The following graphic shows:



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

Answer: C

NEW QUESTION 56
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 59
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 63
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 64
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 66
Fill in the blank: RADIUS protocol uses _____ to communicate with the gateway.

A. UDP
B. TDP
C. CCP
D. HTTP

Answer: A

Explanation: Parameters:

Parameter	Description
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).

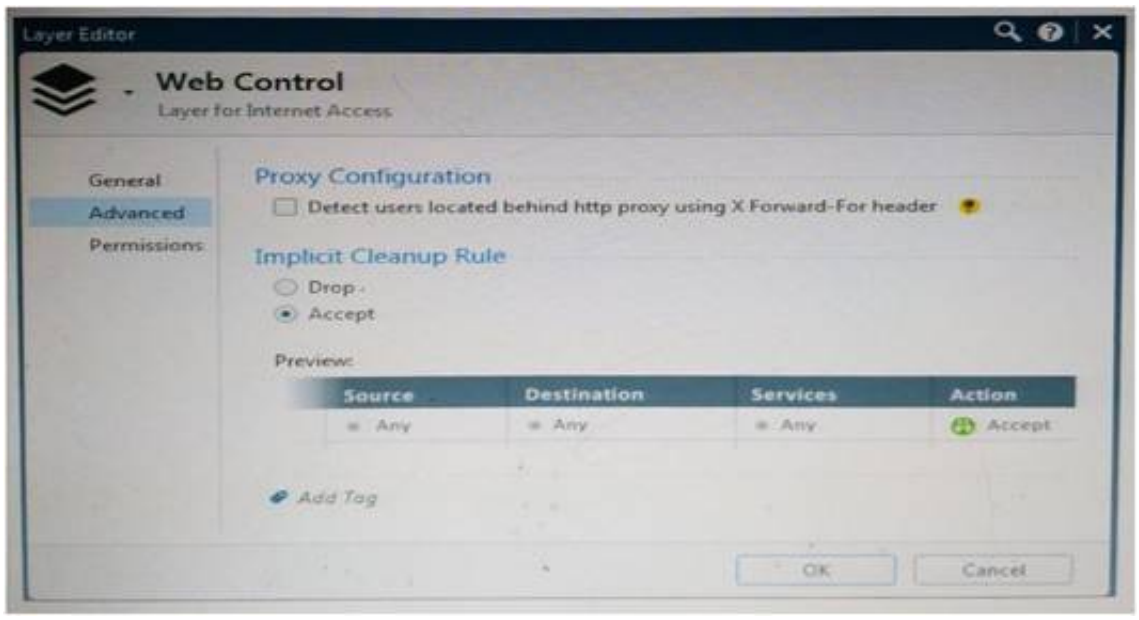
NEW QUESTION 69
In R80 spoofing is defined as a method of:

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.

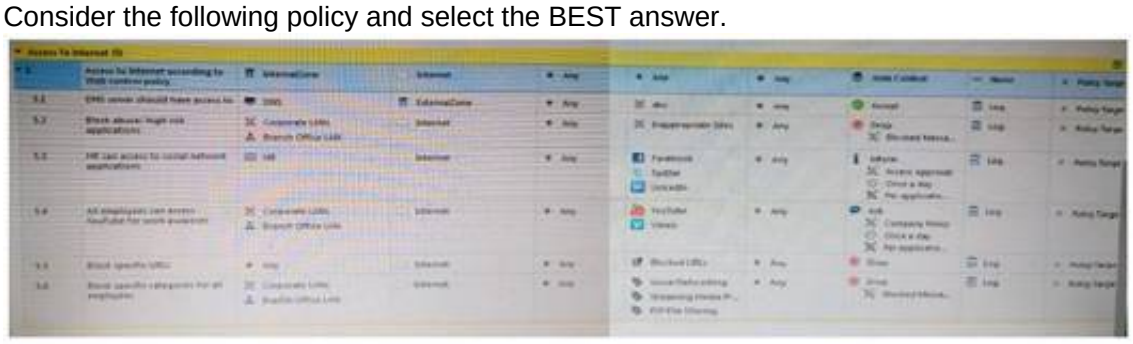
Answer: D

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 71
WeBControl Layer has been set up using the settings in the following dialogue:



Consider the following policy and select the BEST answer.



A. Traffic that does not match any rule in the subpolicy is dropped.
B. All employees can access only Youtube and Vimeo.
C. Access to Youtube and Vimeo is allowed only once a day.
D. Anyone from internal network can access the internet, expect the traffic defined in drop rules 5.2, 5.5 and 5.6.

Answer: D

Explanation: Policy Layers and Sub-Policies
R80 introduces the concept of layers and sub-policies, allowing you to segment your policy according to your network segments or business units/functions. In addition, you can also assign granular privileges by layer or sub-policy to distribute workload and tasks to the most qualified administrators
With layers, the rule base is organized into a set of security rules. These set of rules or layers, are inspected in the order in which they are defined, allowing control over the rule base flow and the security functionalities that take precedence. If an “accept” action is performed across a layer, the inspection will continue to the next layer. For example, a compliance layer can be created to overlay across a cross-section of rules.
Sub-policies are sets of rules that are created for a specific network segment, branch office or business unit, so if a rule is matched, inspection will continue through this subset of rules before it moves on to the next rule.
Sub-policies and layers can be managed by specific administrators, according to their permissions profiles. This facilitates task delegation and workload distribution.

NEW QUESTION 72
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 73
The security Gateway is installed on GAiA R80 The default port for the WEB User Interface is ____.

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

Answer: D

NEW QUESTION 75
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 80
With which command can you view the running configuration of Gaia-based system.

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

Answer: C

NEW QUESTION 83
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 84
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 87
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.

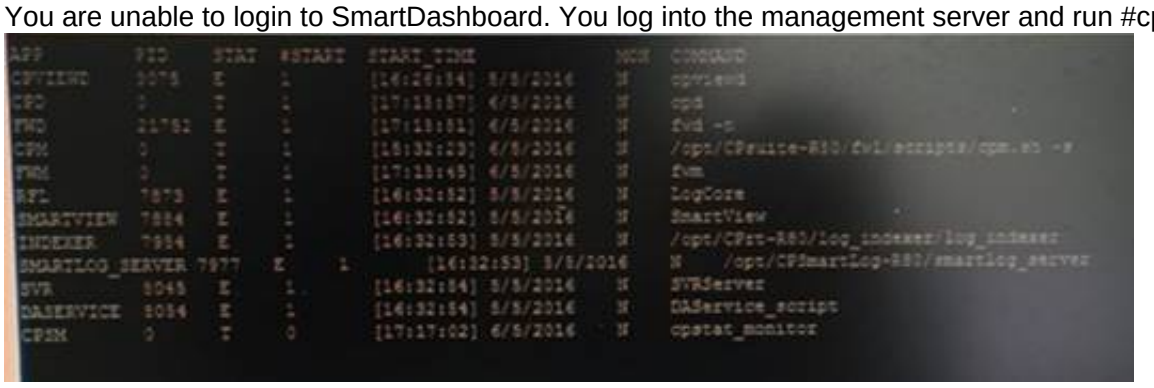
NEW QUESTION 91
Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

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 92
You are unable to login to SmartDashboard. You log into the management server and run #cpwd_admin list with the following output:



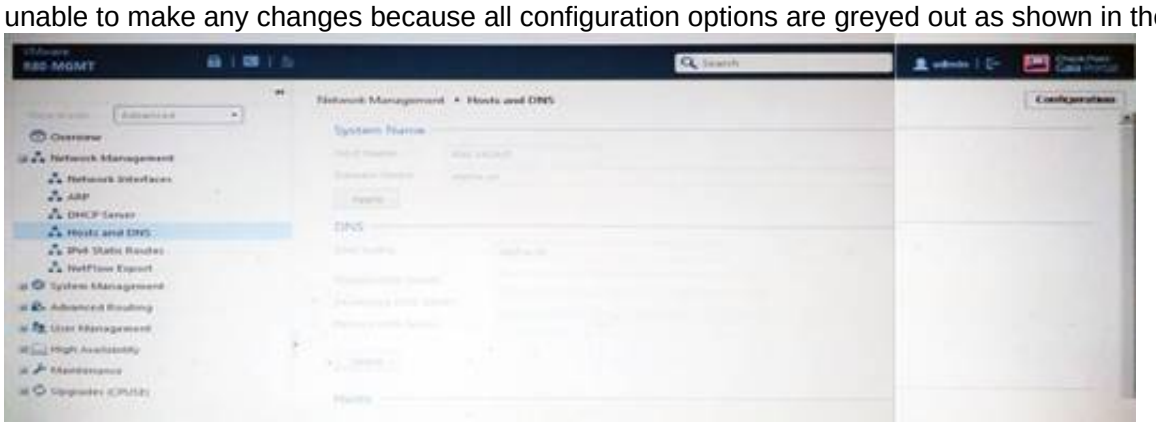
What reason could possibly BEST explain why you are unable to connect to SmartDashboard?

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 97
ABC Corp has a new administrator who logs into the Gaia Portal to make some changes. He realizes that even though he has logged in as an administrator, he is unable to make any changes because all configuration options are greyed out as shown in the screenshot image below. What is the likely cause for this?



A. The Gaia /bin/confd is locked by another administrator from a SmartConsole session.
B. The database is locked by another administrator SSH session.
C. The Network address of his computer is in the blocked hosts.

D. The IP address of his computer is not in the allowed hosts.

Answer: B

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

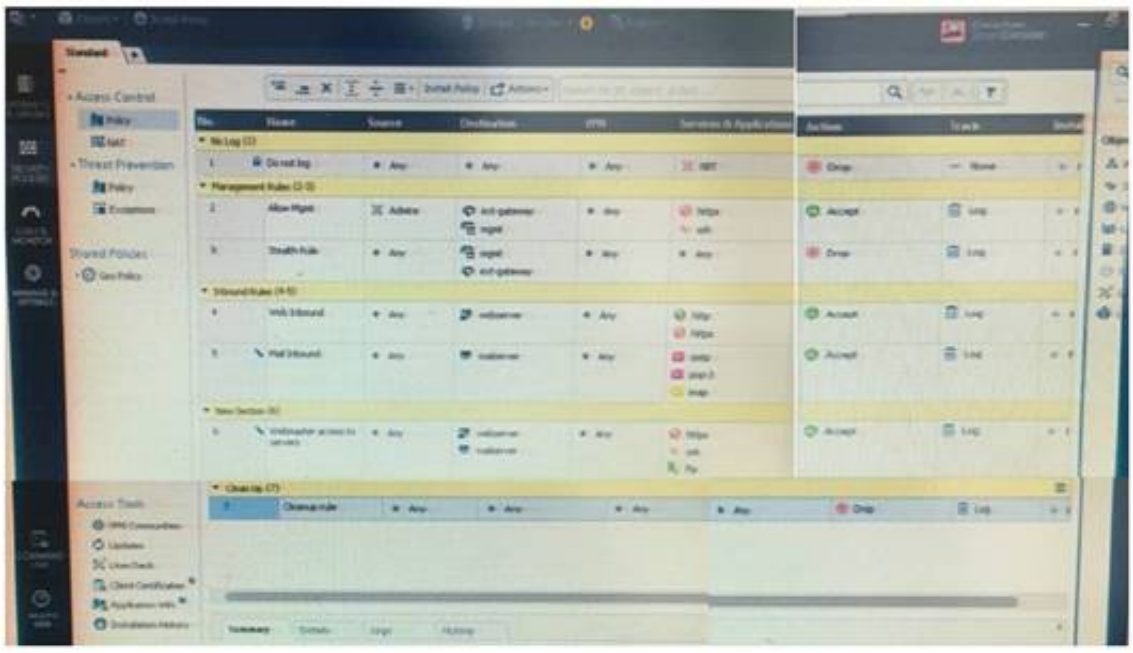
NEW QUESTION 101
What is the default time length that Hit Count Data is kept?

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 105
Examine the following Rule Base.



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

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

Answer: D

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

NEW QUESTION 110
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 114
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

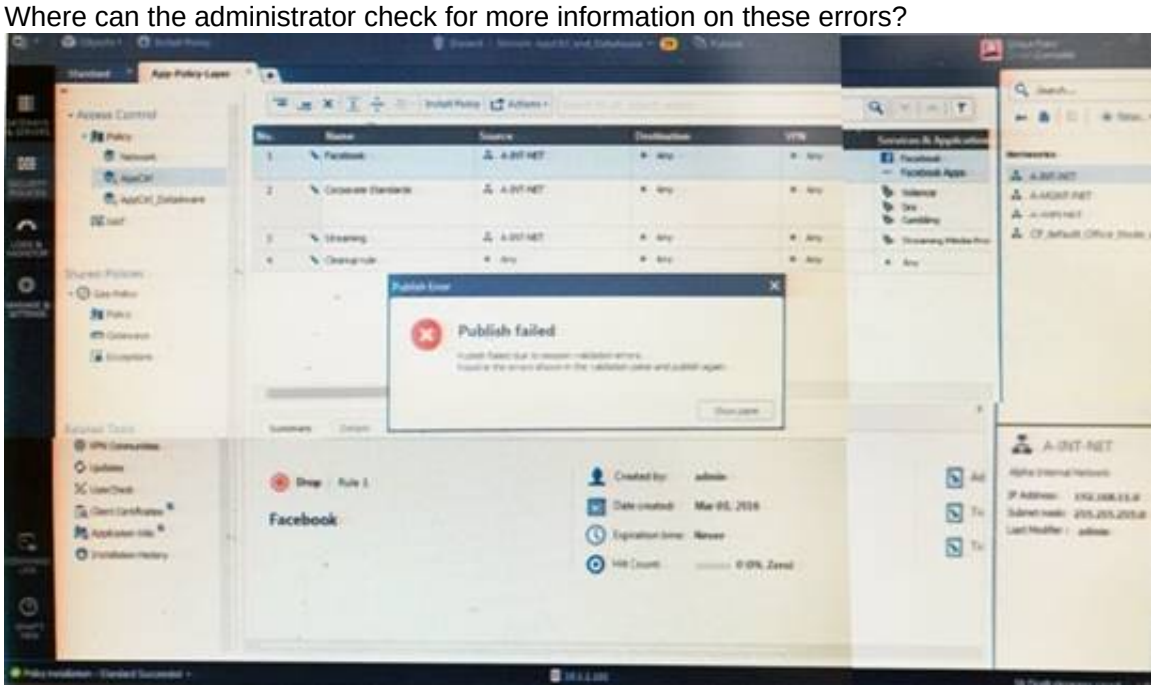
NEW QUESTION 115
What are the two types of address translation rules?

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

Answer: D

Explanation: NAT Rule Base
The NAT Rule Base has two sections that specify how the IP addresses are translated:
Original Packet
Translated Packet References:

NEW QUESTION 118
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 119
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 124
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 127
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 132
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 137
Which of the following is NOT defined by an Access Role object?

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

Answer: D

NEW QUESTION 140
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is ___ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

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

Answer: D

NEW QUESTION 143
Fill in the blanks: The Application Layer Firewalls inspect traffic through the ____ layer(s) of the TCP/IP model and up to and including the ____ layer.

A. Lower; Application
B. First two; Internet
C. First two; Transport
D. Upper; Application

Answer: A

NEW QUESTION 148
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

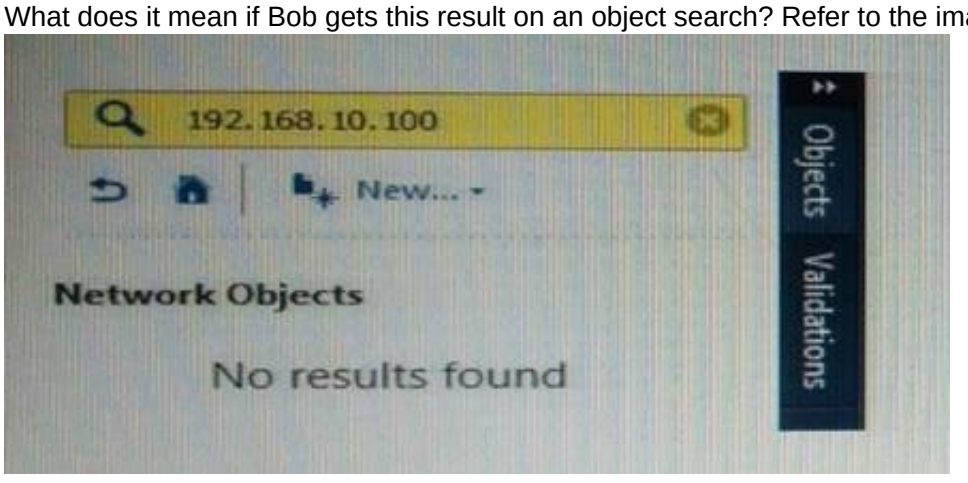
NEW QUESTION 153
Which of the following is NOT an alert option?

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

Answer: B

Explanation: In Action, select:
none - No alert.
log - Sends a log entry to the database.
alert - Opens a pop-up window to your desktop.
mail - Sends a mail alert to your Inbox.
snmptrap - Sends an SNMP alert.
useralert - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert > Alert Commands.

NEW QUESTION 154
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 156
Which of the following is NOT a back up method?

A. Save backup
B. System backup
C. snapshot
D. Migrate

Answer: A

Explanation: The built-in Gaia backup procedures:
Snapshot Management
System Backup (and System Restore)
Save/Show Configuration (and Load Configuration)
Check Point provides three different procedures for backing up (and restoring) the operating system and networking parameters on your appliances.
Snapshot (Revert)
Backup (Restore)
upgrade_export (Migrate) References:

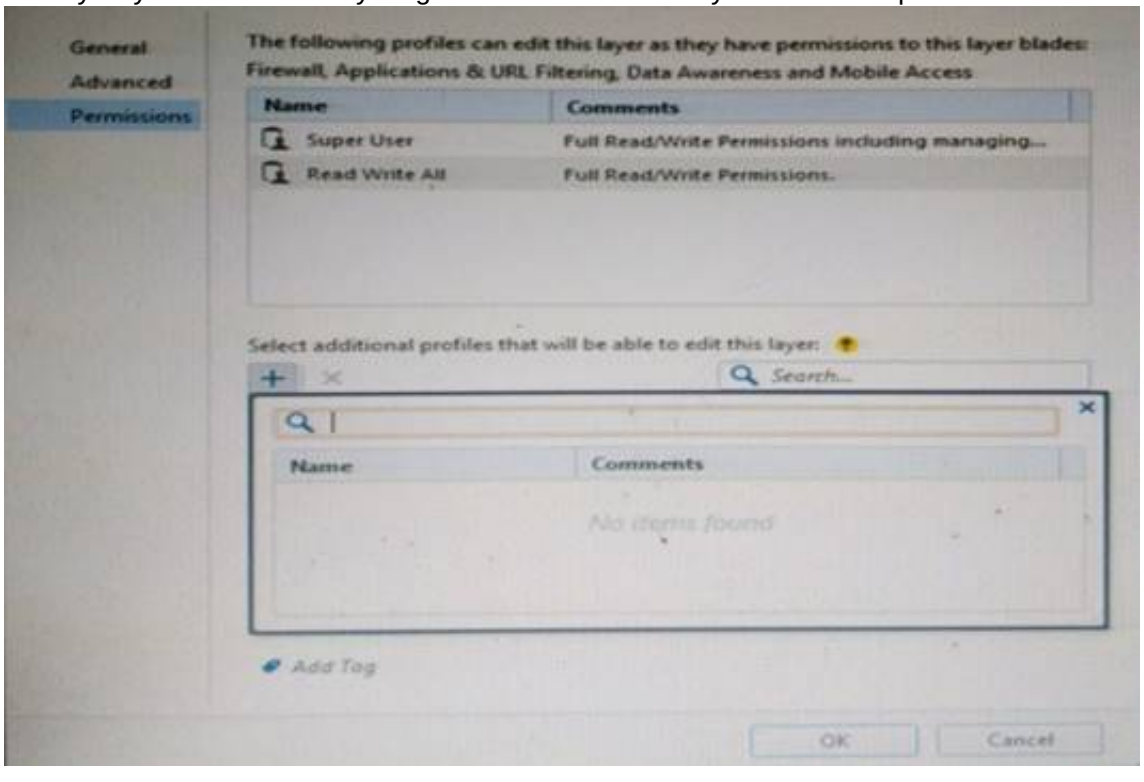
NEW QUESTION 159
Which of the following is NOT a VPN routing option available in a star community?

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 163
You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the “Select additional profile that will be able edit this layer” you do not see anything. What is the most likely cause of this problem? Select the BEST answer.



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

Answer: B

NEW QUESTION 168
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, gateway policy permits access only from Join's desktop which is assigned an IP address 10.0.0.19 via DHCP.
John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but the limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to move around the organization and continue to have access to the HR Web Server. To make this scenario work, the IT administrator:
1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources.
2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.
John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

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

Answer: C

NEW QUESTION 170
Fill in the blank: A ____ is used by a VPN gateway to send traffic as if it were a physical interface.

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

Answer: A

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

NEW QUESTION 171
Which of these components does NOT require a Security Gateway R77 license?

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

Answer: C

NEW QUESTION 176
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 181
Which of the following is TRUE about the Check Point Host object?

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

Answer: A

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

NEW QUESTION 182
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 183
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 185
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 189
Fill in the blanks: A High Availability deployment is referred to as a ____ cluster and a Load Sharing deployment is referred to as a _____ cluster.

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

Answer: D

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

NEW QUESTION 194
Fill in the blank: A(n) _____ rule is created by an administrator and is located before the first and before last rules in the Rule Base.

A. Firewall drop
B. Explicit
C. Implicit accept
D. Implicit drop
E. Implied

Answer: E

Explanation: This is the order that rules are enforced:
First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.
Explicit Rules: These are rules that you create.
Before Last Implied Rules: These implied rules are applied before the last explicit rule.
Last Explicit Rule: We recommend that you use the Cleanup rule as the last explicit rule.
Last Implied Rules: Implied rules that are configured as Last in Global Properties.
Implied Drop Rule: Drops all packets without logging.

NEW QUESTION 197
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 202
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 203
After the initial installation the First Time Configuration Wizard should be run. Select the BEST answer.

A. First Time Configuration Wizard can be run from the Unified SmartConsole.
B. First Time Configuration Wizard can be run from the command line or from the WebUI.
C. First time Configuration Wizard can only be run from the WebUI.
D. Connection to the internet is required before running the First Time Configuration wizard.

Answer: B

Explanation: Check Point Security Gateway and Check Point Security Management require running the First Time Configuration Wizard in order to be configured correctly. The First Time Configuration Wizard is available in Gaia Portal and also through CLI.
To invoke the First Time Configuration Wizard through CLI, run the config_system command from the Exp shell.

NEW QUESTION 204
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 207
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 208
Office mode means that:

A. SecureID client assigns a routable MAC addres
B. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
C. Users authenticate with an Internet browser and use secure HTTPS connection.
D. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
E. Allows a security gateway to assign a remote client an IP addres
F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

Explanation: Office Mode enables a Security Gateway to assign internal IP addresses to SecureClient users. This IP address will not be exposed to the public network, but is encapsulated inside the VPN tunnel between the client and the Gateway. The IP to be used externally should be assigned to the client in the usual way by the Internet Service provider used for the Internet connection. This mode allows a Security Administrator to control which addresses are used by remote clients inside the local network and makes them part of the local network. The mechanism is based on an IKE protocol extension through which the Security Gateway can send an internal IP address to the client.

NEW QUESTION 212
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 214
Choose the SmartLog property that is TRUE.

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

Answer: D

NEW QUESTION 215
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 220
Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

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

Answer: D

Explanation: Users
Use the WebUI and CLI to manage user accounts. You can:
Add users to your Gaia system.
Edit the home directory of the user.
Edit the default shell for a user.
Give a password to a user.
Give privileges to users.

NEW QUESTION 223
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 227
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 230
Which policy type is used to enforce bandwidth and traffic control rules?

A. Threat Emulation
B. Access Control
C. QoS
D. Threat Prevention

Answer: C

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

NEW QUESTION 234
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 235
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 240
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 244
NAT can NOT be configured on which of the following objects?

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

Answer: A

NEW QUESTION 248
The Captive Portal tool:

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

Answer: A

NEW QUESTION 250
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 252
Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

A. SmartMonitor
B. SmartView Web Application
C. SmartReporter

D. SmartTracker

Answer: B

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

NEW QUESTION 257
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 261
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 264
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 265
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 266
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 269
Which of the following statements accurately describes the command snapshot?

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

Answer: A

NEW QUESTION 270
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 272
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 276
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 281
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 286
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 288
Fill in the blank: Licenses can be added to the License and Contract repository _____.

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

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

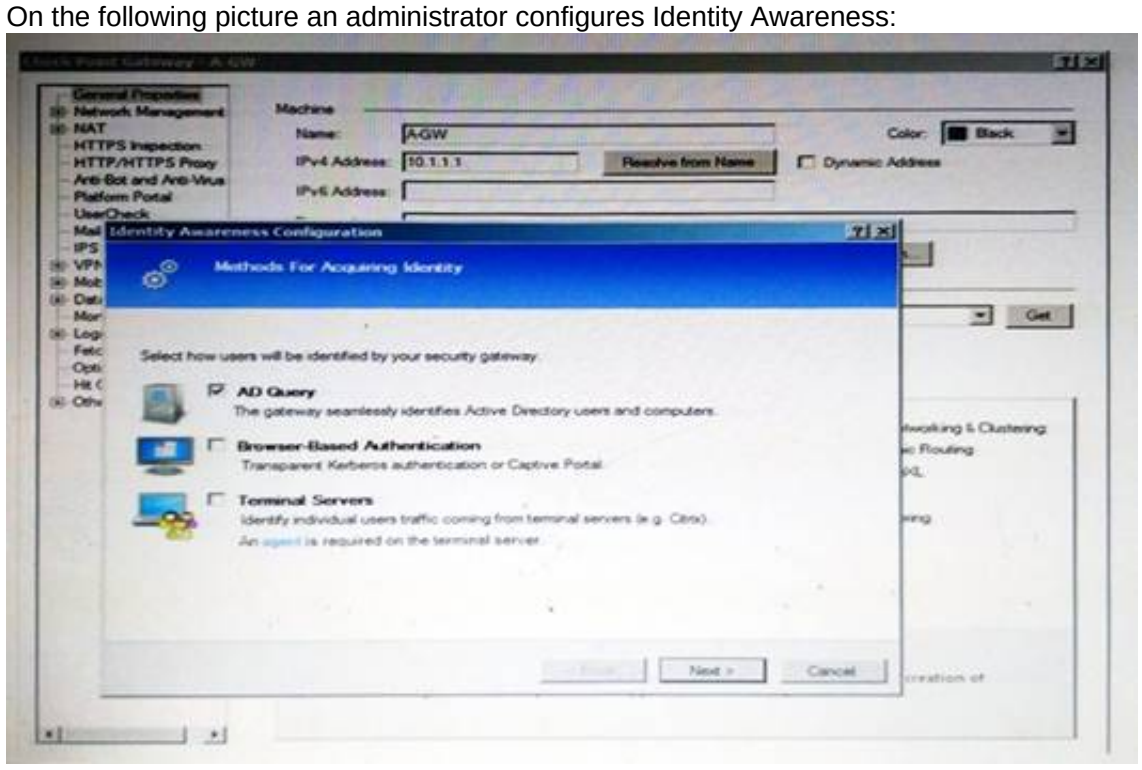
Answer: A

NEW QUESTION 289
When using LDAP as an authentication method for Identity Awareness, the query:

A. Requires client and server side software.
B. Prompts the user to enter credentials.
C. Requires administrators to specifically allow LDAP traffic to and from the LDAP Server and the Security Gateway.
D. Is transparent, requiring no client or server side software, or client intervention.

Answer: D

NEW QUESTION 290
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 294
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 298
Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.

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

Answer: A

NEW QUESTION 299
You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?

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

Answer: C

Explanation: 2. Snapshot Management
The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.
Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.
The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

NEW QUESTION 300
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 301
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 304
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 307
Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

A. Change the Rule Base and install the Policy to all Security Gateways
B. Block Intruder feature of SmartView Tracker
C. Intrusion Detection System (IDS) Policy install
D. SAM – Suspicious Activity Rules feature of SmartView Monitor

Answer: B

NEW QUESTION 312
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 316
What component of R80 Management is used for indexing?

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

Answer: D

NEW QUESTION 319
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 322
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 325
A Cleanup rule:

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

Answer: A

NEW QUESTION 328
An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).
Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.
If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.
Which of the following is the BEST Explanation: for this behavior?

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

Answer: C

NEW QUESTION 332
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 336
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 338
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 343
The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

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

Answer: D

NEW QUESTION 346
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 347
Match the following commands to their correct function. Each command has one function only listed.

Command	Function
C1 cp_admin_convert	F1: export and import different revisions of the database.
C2 cpca_client	F2: export and import policy package
C3 cp_merge	F3: transfer Log data to an external database.
C4 cpwd_admin	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard.

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

Answer: A

NEW QUESTION 350
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 353
Review the rules. Assume domain UDP is enabled in the implied rules.

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:

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

Answer: D

NEW QUESTION 357
Which of the following is NOT an option for internal network definition of Anti-spoofing?

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

Answer: B

NEW QUESTION 362
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 363
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 367
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 371
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.
John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his desktop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.
To make this scenario work, the IT administrator:
1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.
3) Changes from static IP address to DHCP for the client PC.
What should John request when he cannot access the web server from his laptop?

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

Answer: C

NEW QUESTION 375
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 379
A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

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

Answer: B

NEW QUESTION 384
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

A. Dropped without sending a negative acknowledgment
B. Dropped without logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment

Answer: D

NEW QUESTION 389
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 394
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 397
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 400
You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

A. Manual copies of the directory $FWDIR/conf
B. upgrade_export command
C. Database Revision Control
D. GAiA backup utilities

Answer: C

NEW QUESTION 402
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 407
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 412
You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

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

Answer: B

NEW QUESTION 416
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 418
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 421
Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

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

Answer: D

NEW QUESTION 423
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 427
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 429
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 430
Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

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

Answer: A

NEW QUESTION 435
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 437
You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After a while, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

A. Run fwm dbexport -1 filenam
B. Restore the databas
C. Then, run fwm dbimport -1 filename to import the users.
D. Run fwm_dbexport to export the user databas

E. Select restore the entire database in the Database Revision scree
F. Then, run fwm_dbimport.
G. Restore the entire database, except the user database, and then create the new user and user group.
H. Restore the entire database, except the user database.

Answer: D

NEW QUESTION 441
MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway.
How do you apply the license?

A. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.
B. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.
C. Using the remote Gateway's IP address, and applying the license locally with command cplic put.
D. Using each of the Gateway's IP addresses, and applying the licenses on the Security Management Server with the command cprlic put.

Answer: B

NEW QUESTION 445
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 450
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 455
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 459
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 464
What is the benefit of Manual NAT over Automatic NAT?

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

Answer: C

NEW QUESTION 465
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 470
Which tool CANNOT be launched from SmartUpdate R77?

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

Answer: B

NEW QUESTION 473
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 474
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 477
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 478
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 479
What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security Gateway?

A. In Global Properties > Reporting Tools check the box Enable tracking all rules (including rules marked as None in the Track column). Send these logs to a secondary log server for a complete logging histor
B. Use your normal log server for standard logging for troubleshooting.
C. Install the View Implicit Rules package using SmartUpdate.
D. Define two log servers on the R77 Gateway objec
E. Lof Implied Rules on the first log serve
F. Enable Log Rule Base on the second log serve
G. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits.
H. Check the Log Implied Rules Globally box on the R77 Gateway object.

Answer: A

Explanation: Topic 4, Exam Pool D

NEW QUESTION 482
Which of the following commands is used to verify license installation?

A. Cplic verify license

B. Cplic print
C. Cplic show
D. Cplic license

Answer: B

NEW QUESTION 485
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 489
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 494
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 498
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 499
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 500
Which one of the following is TRUE?

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

Answer: C

NEW QUESTION 502
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

A. fwd
B. fwm

C. cpd
D. cpwd

Answer: B

NEW QUESTION 503
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

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

Answer: A

NEW QUESTION 504
Which identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

A. ADQuery
B. Terminal Servers Endpoint Identity Agent
C. Endpoint Identity Agent and Browser-Based Authentication
D. RADIUS and Account Logon

Answer: D

NEW QUESTION 506
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

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

Answer: C

NEW QUESTION 509
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 514
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 515
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 517
When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

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

Answer: D

NEW QUESTION 520
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 521
Which two of these Check Point Protocols are used by ?

A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG

Answer: B

NEW QUESTION 526
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 527
In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

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

Answer: C

NEW QUESTION 532
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 537
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 539
When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

A. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
B. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
C. The entire Management Database and all sessions and other administrators can connect only as Read-only.
D. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.

Answer: D

NEW QUESTION 541

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 543
Which of the following is NOT an option to calculate the traffic direction?

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

Answer: D

NEW QUESTION 545
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 548
The SIC Status “Unknown” means

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

Answer: AC

Explanation: After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:
Communicating - The secure communication is established.
Unknown - There is no connection between the gateway and Security Management Server.
Not Communicating - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

NEW QUESTION 550
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 551
How would you determine the software version from the CLI?

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

Answer: A

NEW QUESTION 556
Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.

A. SHA-256
B. SHA-200
C. MD5
D. SHA-128

Answer: A

NEW QUESTION 558
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 559
Fill the blank. IT is Best Practice to have a _____ rule at the end of each policy layer.

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

Answer: A

NEW QUESTION 564
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 565
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 568
Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 571
Which firewall daemon is responsible for the FW CLI commands?

A. fwd
B. fwm
C. cpm
D. cpd

Answer: A

NEW QUESTION 576
Fill in the blanks. There are _____ types of software containers _____

A. Three; security managemen
B. Security Gateway and endpoint security.

C. Three; Security Gateway, endpoint Security, and gateway management.
D. Two; security management and endpoint security
E. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 579
When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

A. Distributed
B. Standalone
C. Bridge

Answer: A

NEW QUESTION 583
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

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

Answer: C

NEW QUESTION 584
You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

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

Answer: A

NEW QUESTION 585
What protocol is specifically used for clustered environments?

A. Clustered Protocol
B. Synchronized Cluster Protocol
C. Control Cluster Protocol
D. Cluster Control Protocol

Answer: D

NEW QUESTION 586
Access roles allow the firewall administrator to configure Network access according to:

A. a combination of computer or computer groups and network
B. users and user groups
C. all of above
D. remote access clients

Answer: C

NEW QUESTION 589
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

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

Answer: D

NEW QUESTION 593
When an encrypted packet is decrypted, where does this happen?

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

Answer: A

NEW QUESTION 595
When using Monitored circuit VRRP, what is a priority delta?

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

Answer: C

NEW QUESTION 599
Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

A. All options stop Check Point processes
B. backup
C. migrate export
D. snapshot

Answer: D

NEW QUESTION 600
Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

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

Answer: D

NEW QUESTION 601
Which repositories are installed on the Security Management Server by SmartUpdate?

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

Answer: D

NEW QUESTION 606
What is the difference between SSL VPN and IPSec VPN?

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

Answer: D

NEW QUESTION 610
Fill in the blank: In order to install a license, it must first be added to the _____ .

A. User Center
B. Package repository
C. Download Center Web site
D. License and Contract repository

Answer: B

NEW QUESTION 611
Fill in the blanks. In _____ NAT, the _____ is translated.

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

Answer: B

NEW QUESTION 615
Which of the following is NOT a method used by Identity Awareness for acquiring identity?

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

Answer: D

NEW QUESTION 619
Fill in the blank: Service blades must be attached to a _____ .

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

Answer: A

NEW QUESTION 622
In the Check Point Security Management Architecture, which component(s) can store logs?

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

Answer: B

NEW QUESTION 626
Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

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

Answer: B

NEW QUESTION 627
.....

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