Check-Point

Exam Questions 156-215.80

Check Point Certified Security Administrator

NEW QUESTION 1
- (Exam Topic 1)
Which of the following commands can be used to remove site-to-site IPSEC Security Associations (SA)?

A. vpn tu
B. vpn ipsec remove -l
C. vpn debug ipsec
D. fw ipsec tu

Answer: A

Explanation:
vpn tu
Description Launch the TunnelUtil tool which is used to control VPN tunnels.
Usage vpn tu vpn tunnelutil Example vpn tu Output

```
**********     Select Option     **********


(1)             List all IKE SAs

(2)             List all IPsec SAs

(3)             List all IKE SAs for a given peer (GW) or user (Client)

(4)             List all IPsec SAs for a given peer (GW) or user (Client)

(5)             Delete all IPsec SAs for a given peer (GW)

(6)             Delete all IPsec SAs for a given User (Client)

(7)             Delete all IPsec+IKE SAs for a given peer (GW)

(8)             Delete all IPsec+IKE SAs for a given User (Client)

(9)             Delete all IPsec SAs for ALL peers and users

(0)             Delete all IPsec+IKE SAs for ALL peers and users


(Q)             Quit
```

NEW QUESTION 2
- (Exam Topic 1)
Which of the following is NOT a component of a Distinguished Name?

A. Organization Unit
B. Country
C. Common name
D. User container

Answer: D

Explanation:
Distinguished Name Components
CN=common name, OU=organizational unit, O=organization, L=locality, ST=state or province, C=country name

NEW QUESTION 3
- (Exam Topic 1)
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 4
- (Exam Topic 1)
Which utility allows you to configure the DHCP service on GAIA from the command line?

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

Answer: C

Explanation:
Sysconfig Configuration Options

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

NEW QUESTION 5
- (Exam Topic 1)
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 6
- (Exam Topic 1)
You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

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

Answer: D

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

NEW QUESTION 7
- (Exam Topic 1)
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

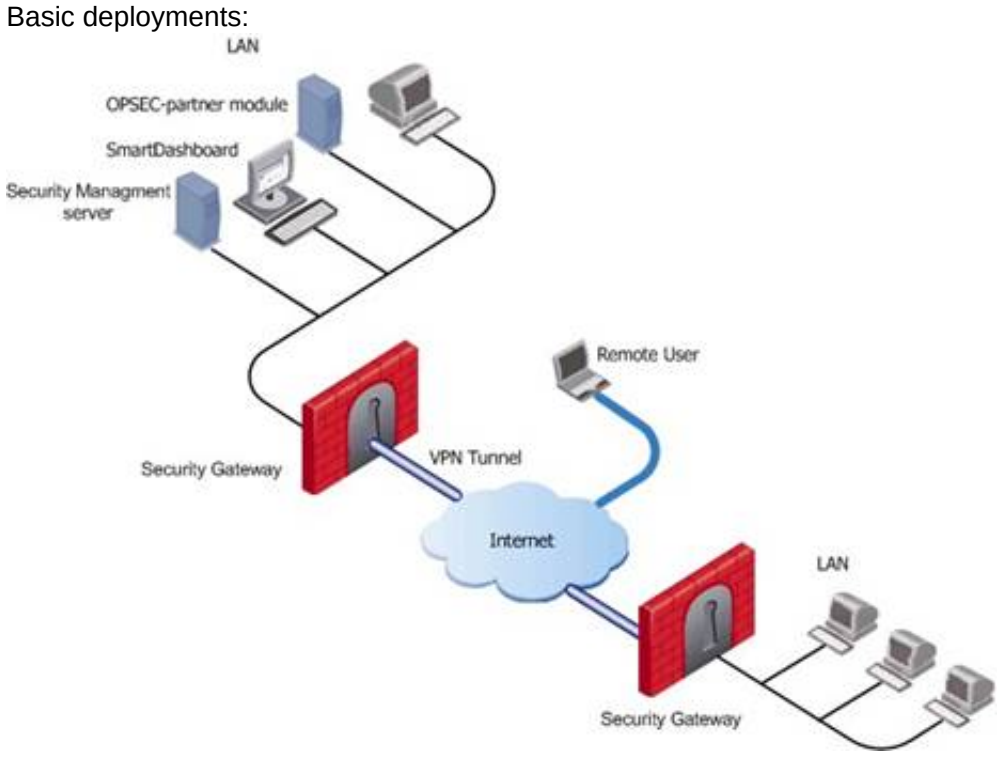
NEW QUESTION 8
- (Exam Topic 1)
What are the three essential components of the Check Point Security Management Architecture?

A. SmartConsole, Security Management Server, Security Gateway
B. SmartConsole, SmartUpdate, Security Gateway
C. Security Management Server, Security Gateway, Command Line Interface
D. WebUI, SmartConsole, Security Gateway

Answer: A

Explanation:
Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.

Distributed deployment - Security Gateway and the Security Management server are installed on different machines.
Deployments
Basic deployments:



Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.
You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.
The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.
There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.

NEW QUESTION 9
- (Exam Topic 1)
By default, which port does the WebUI listen on?

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

Answer: C

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

NEW QUESTION 10
- (Exam Topic 1)
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 1)
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 14
- (Exam Topic 1)
Which default user has full read/write access?

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

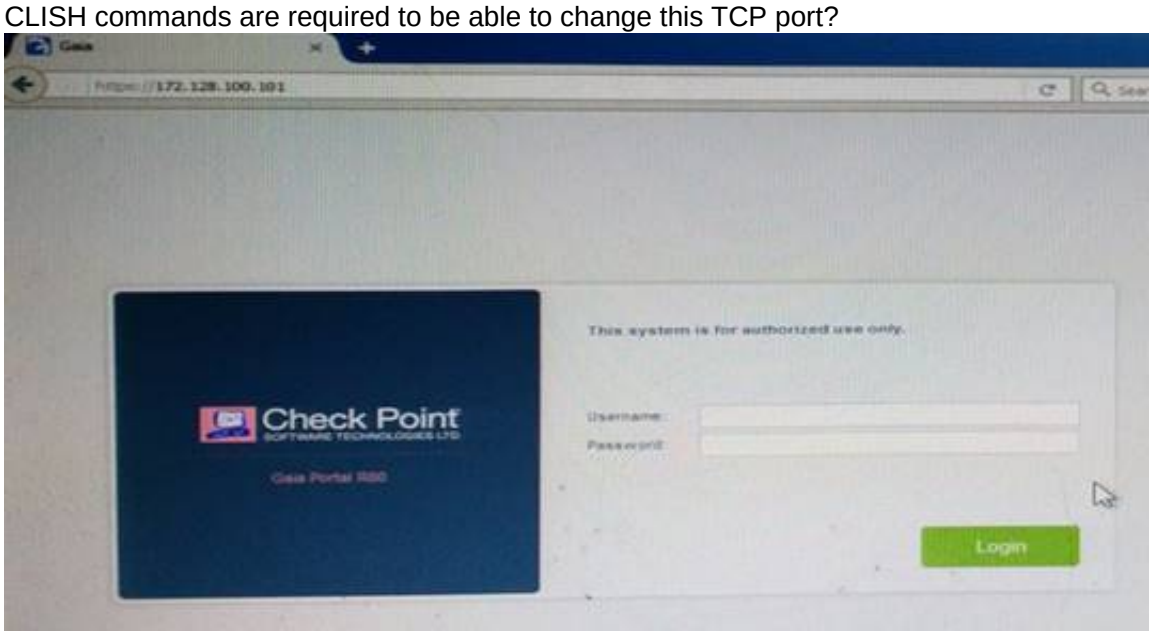
Answer: C

NEW QUESTION 18
- (Exam Topic 1)
Which of the following is TRUE regarding Gaia command line?

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

Answer: D

NEW QUESTION 23
- (Exam Topic 1)
Kofi, the administrator of the ABC Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



A. set web ssl-port <new port number>
B. set Gaia-portal <new port number>
C. set Gaia-portal https-port <new port number>
D. set web https-port <new port number>

Answer: A

Explanation:
In Clish
Connect to command line on Security Gateway / each
Log in to Clish.
Set the desired port (e.g., port 4434):
Cluster member.
HostName> set web ssl-port <Port_Number>
Save the changes:
HostName> save config
Verify that the configuration was saved:
[Expert@HostName]# grep 'httpd:ssl_port' /config/db/initial References:

NEW QUESTION 26
- (Exam Topic 1)
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 31
- (Exam Topic 1)
Fill in the blank: To build an effective Security Policy, use a _____ and _____ rule.

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

Answer: A

NEW QUESTION 35
- (Exam Topic 1)
You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

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

Answer: B

NEW QUESTION 40
- (Exam Topic 1)
What is the default shell for the command line interface?

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

Answer: B

Explanation:
The default shell of the CLI is called clish References:

NEW QUESTION 41
- (Exam Topic 1)
DLP and Geo Policy are examples of what type of Policy?

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

Answer: B

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

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

NEW QUESTION 42
- (Exam Topic 1)
ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house R80 Management to the other administrators in ABC Corp.

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

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

Answer: C

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

NEW QUESTION 46
- (Exam Topic 1)
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

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

Answer: A

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

NEW QUESTION 48
- (Exam Topic 1)
What is the purpose of Captive Portal?

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

Answer: C

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

NEW QUESTION 53
- (Exam Topic 1)
Review the following screenshot and select the BEST answer.

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

Answer: C

NEW QUESTION 57
- (Exam Topic 1)
Joey wants to configure NTP on R80 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

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

Answer: A

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

NEW QUESTION 61
- (Exam Topic 1)
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 63
- (Exam Topic 1)
Which type of the Check Point license ties the package license to the IP address of the Security Management Server?

A. Local
B. Central
C. Corporate
D. Formal

Answer: B

NEW QUESTION 68
- (Exam Topic 1)
Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

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

Answer: D

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

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 72
- (Exam Topic 1)
Choose what BEST describes the Policy Layer Traffic Inspection.

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

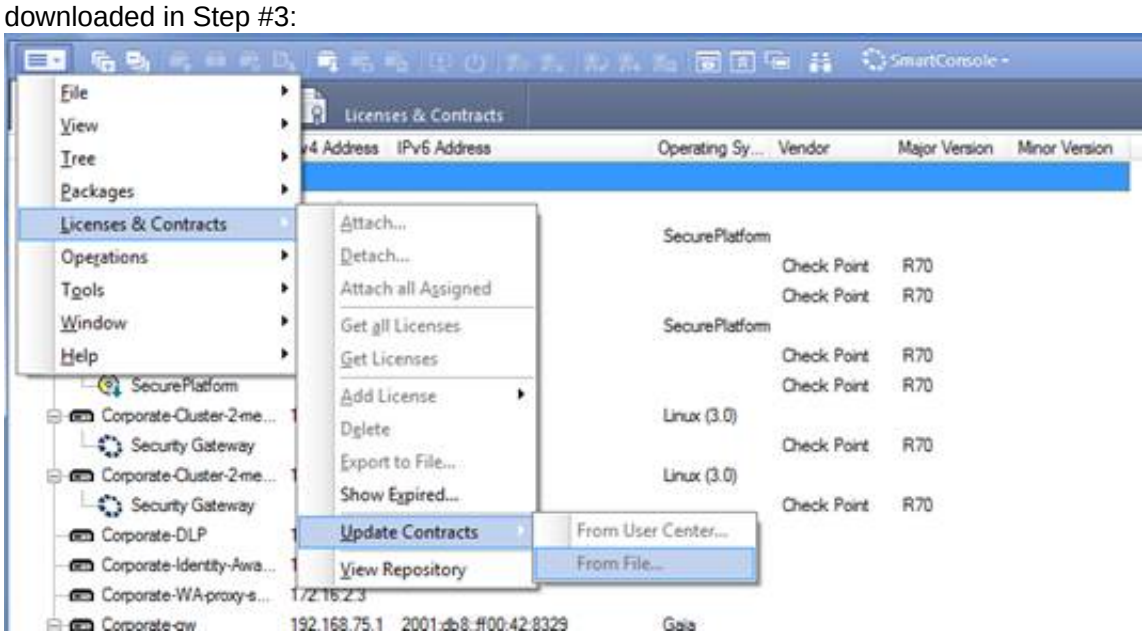
Answer: B

NEW QUESTION 77
- (Exam Topic 1)
Which application should you use to install a contract file?

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

Answer: C

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



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

NEW QUESTION 78
- (Exam Topic 1)
Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

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

Answer: D

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

NEW QUESTION 79
- (Exam Topic 1)
Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

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

Answer: C

NEW QUESTION 81
- (Exam Topic 1)
Which utility shows the security gateway general system information statistics like operating system information and resource usage, and individual software blade statistics of VPN, Identity Awareness and DLP?

A. cpconfig
B. fw ctl pstat
C. cpview
D. fw ctl multik stat

Answer: C

Explanation:
CPView Utility is a text based built-in utility that can be run ('cpview' command) on Security Gateway / Security Management Server / Multi-Domain Security Management Server. CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway). The data is continuously updated in easy to access views.

NEW QUESTION 83
- (Exam Topic 1)
Fill in the blank: The ____ is used to obtain identification and security information about network users.

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

Answer: A

NEW QUESTION 87
- (Exam Topic 1)
An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret is shared and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

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

Answer: C

NEW QUESTION 90
- (Exam Topic 1)
Which of the following is NOT a license activation method?

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

Answer: A

NEW QUESTION 91
- (Exam Topic 1)
In R80, Unified Policy is a combination of

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

Answer: D

Explanation:
D is the best answer given the choices. Unified Policy
In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:
Firewall and VPN
Application Control and URL Filtering
Identity Awareness
Data Awareness
Mobile Access
Security Zones

NEW QUESTION 94
- (Exam Topic 1)
Which one of the following is the preferred licensing model? Select the Best answer.

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

Answer: B

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

NEW QUESTION 99
- (Exam Topic 1)
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 100
- (Exam Topic 1)
On the following graphic, you will find layers of policies.

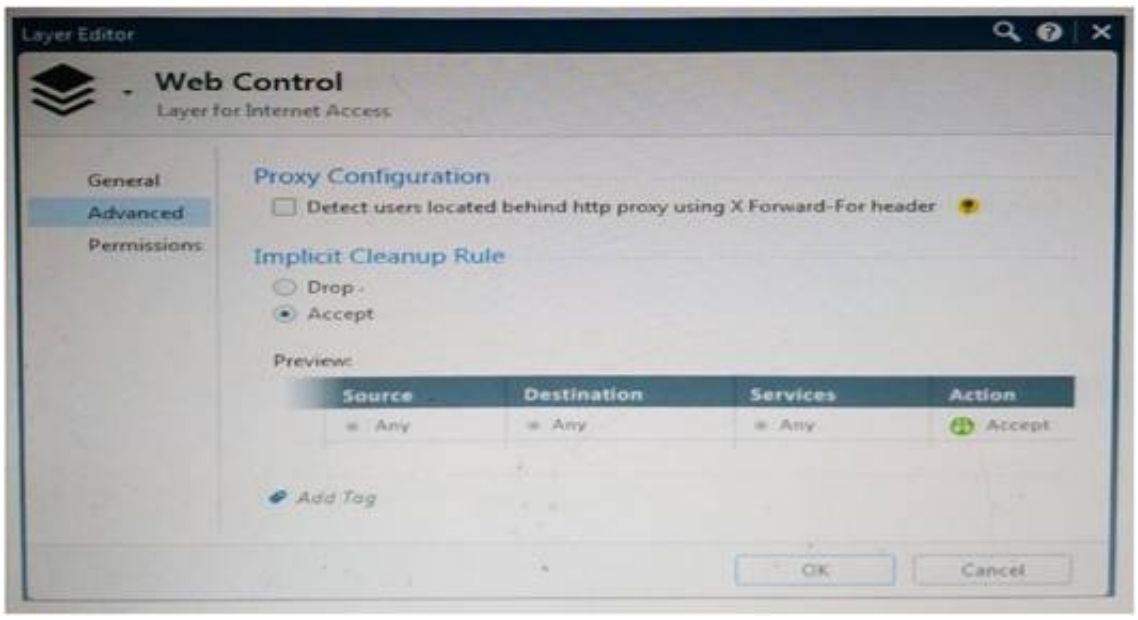
What is a precedence of traffic inspection for the defined polices?

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

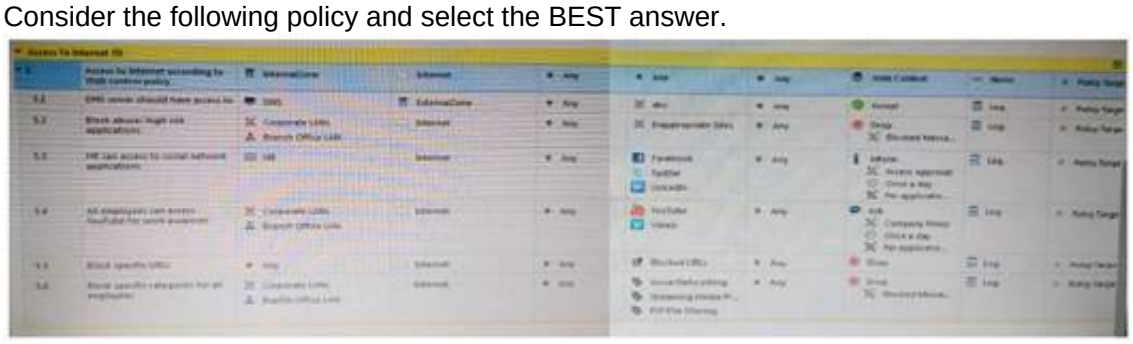
Answer: B

Explanation:
To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.
For example, when you upgrade to R80 from earlier versions:
Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.
When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.
Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.
All layers are evaluated in parallel
When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.
All layers are evaluated in parallel

NEW QUESTION 101
- (Exam Topic 1)
WeBControl Layer has been set up using the settings in the following dialogue:



Consider the following policy and select the BEST answer.



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

Answer: D

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

NEW QUESTION 106
- (Exam Topic 1)
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 109
- (Exam Topic 1)
Fill in the blank: The ____ collects logs and sends them to the ____.

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

Answer: D

NEW QUESTION 111
- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 115
- (Exam Topic 1)
Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when ____.

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

Answer: A

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

NEW QUESTION 119
- (Exam Topic 1)
What are the three conflict resolution rules in the Threat Prevention Policy Layers?

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

Answer: C

NEW QUESTION 124
- (Exam Topic 1)
Where can you trigger a failover of the cluster members?
Log in to Security Gateway CLI and run command clusterXL_admin down.
In SmartView Monitor right-click the Security Gateway member and select Cluster member stop. Log into Security Gateway CLI and run command cphaprob down.

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

Answer: C

Explanation:
How to Initiate Failover

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 125
- (Exam Topic 1)
What is NOT an advantage of Packet Filtering?

A. Low Security and No Screening above Network Layer
B. Application Independence
C. High Performance
D. Scalability

Answer: A

Explanation:
Packet Filter Advantages and Disadvantages

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

NEW QUESTION 130
- (Exam Topic 1)
Harriet wants to protect sensitive information from intentional loss when users browse to a specific URL: https://personal.mymail.com, which blade will she enable to achieve her goal?

A. DLP
B. SSL Inspection
C. Application Control
D. URL Filtering

Answer: A

Explanation:
Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies—protecting sensitive corporate information from both intentional and unintentional loss.

NEW QUESTION 131
- (Exam Topic 1)
To optimize Rule Base efficiency, the most hit rules should be where?

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

Answer: C

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

NEW QUESTION 132
- (Exam Topic 1)
Which feature is NOT provided by all Check Point Mobile Access solutions?

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

Answer: A

Explanation:
Types of Solutions
Enterprise-grade, secure connectivity to corporate resources.
Strong user authentication.
Granular access control. References:

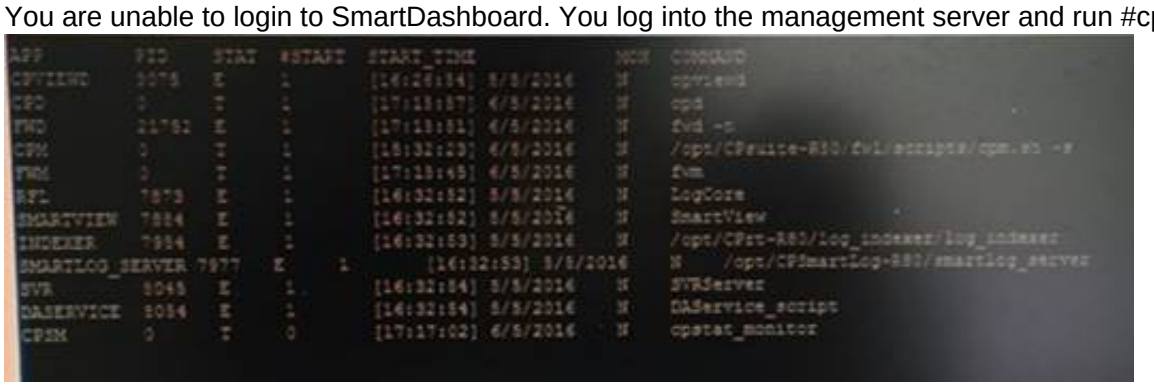
NEW QUESTION 134
- (Exam Topic 1)
Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

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

Answer: C

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

NEW QUESTION 136
- (Exam Topic 1)
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"

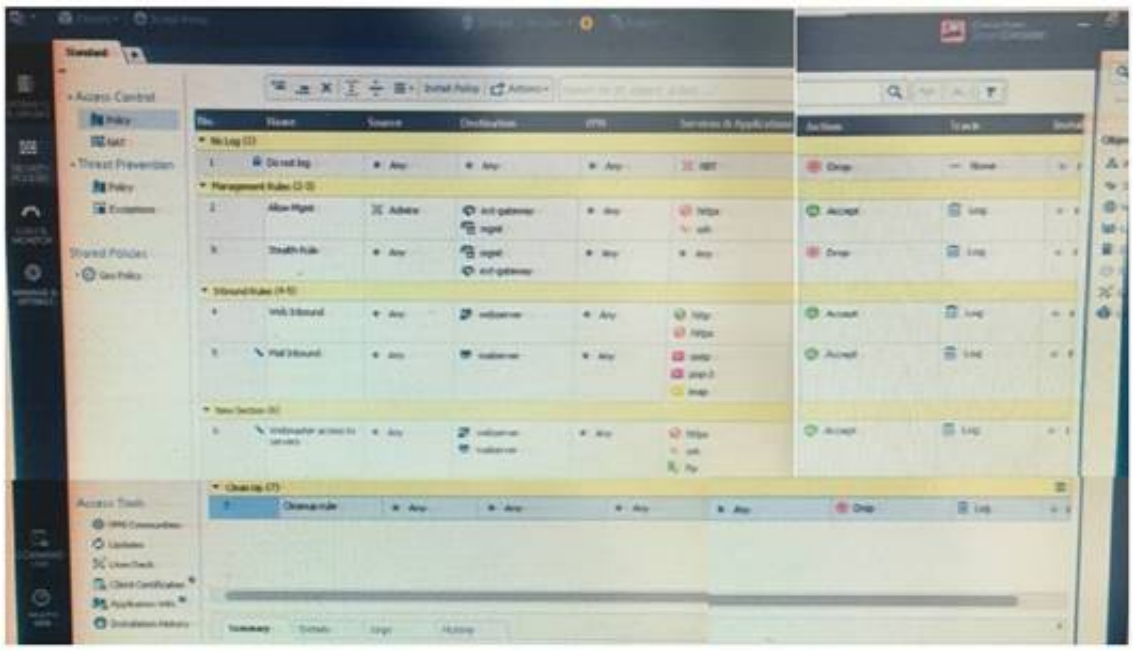
NEW QUESTION 137
- (Exam Topic 1)
What is the default time length that Hit Count Data is kept?

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

Answer: A

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

NEW QUESTION 139
- (Exam Topic 1)
Examine the following Rule Base.



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

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

Answer: D

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

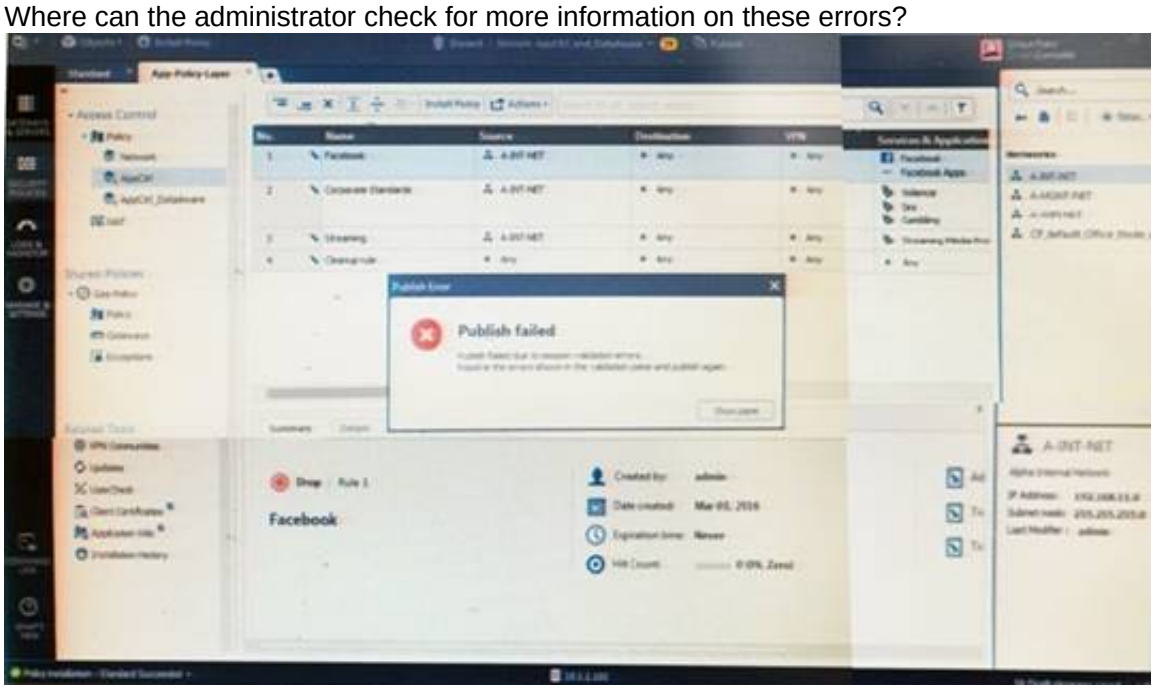
NEW QUESTION 142
- (Exam Topic 1)
Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?

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 147
- (Exam Topic 1)
Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.
Where can the administrator check for more information on these errors?



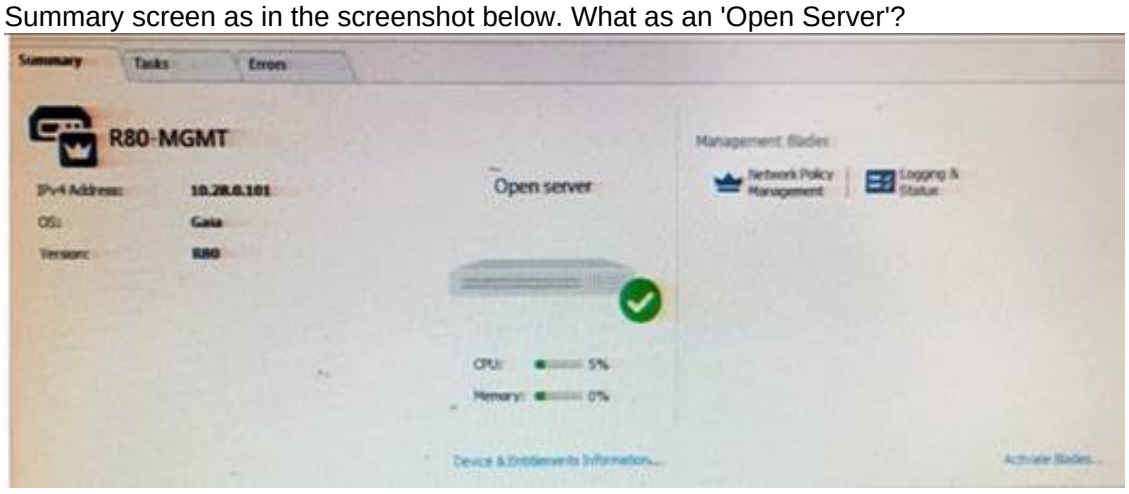
A. The Log and Monitor section in SmartConsole
B. The Validations section in SmartConsole
C. The Objects section in SmartConsole
D. The Policies section in SmartConsole

Answer: B

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

NEW QUESTION 151
- (Exam Topic 1)
Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the

Summary screen as in the screenshot below. What as an 'Open Server'?



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

Answer: A

Explanation:

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

NEW QUESTION 155
- (Exam Topic 2)
What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

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

Answer: A

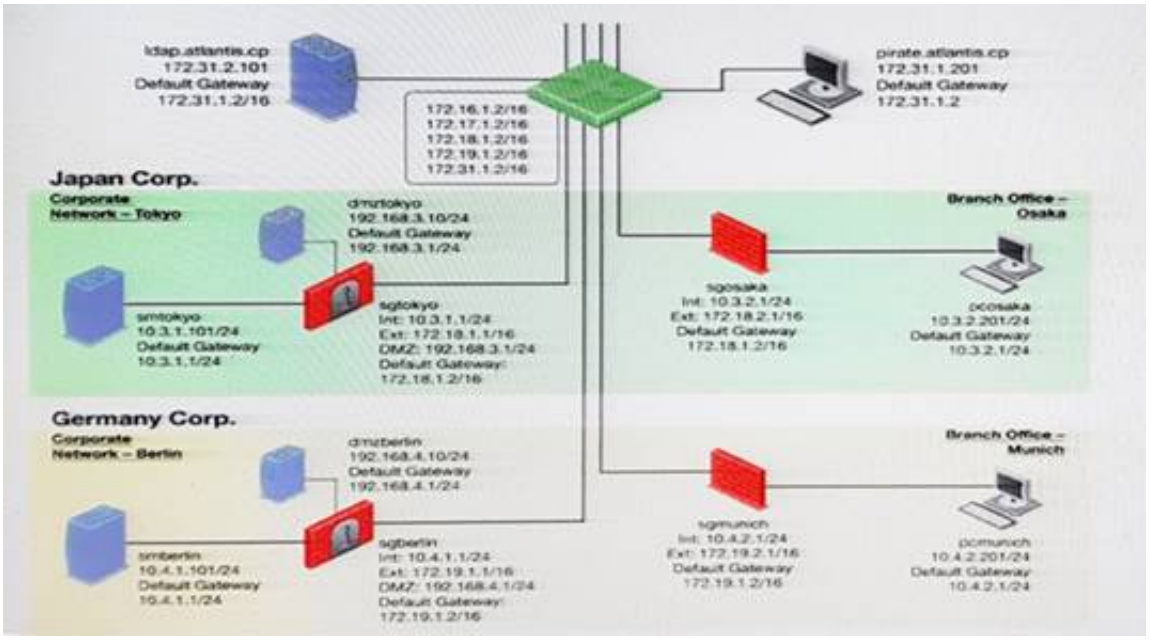
NEW QUESTION 157
- (Exam Topic 2)
Provide very wide coverage for all products and protocols, with noticeable performance impact.

How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

A. Set High Confidence to Low and Low Confidence to Inactive.
B. Set the Performance Impact to Medium or lower.
C. The problem is not with the Threat Prevention Profil
D. Consider adding more memory to the appliance.
E. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B

NEW QUESTION 162
- (Exam Topic 2)
You want to reset SIC between smberlin and sgosaka.



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

What is the reason for this behavior?

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

Answer: C

NEW QUESTION 167
- (Exam Topic 2)
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 170
- (Exam Topic 2)
What statement is true regarding Visitor Mode?

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

Answer: A

NEW QUESTION 173
- (Exam Topic 2)
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is ___ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

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

Answer: D

NEW QUESTION 174
- (Exam Topic 2)
What are the three tabs available in SmartView Tracker?

A. Network & Endpoint, Management, and Active

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

Answer: C

NEW QUESTION 175
- (Exam Topic 2)
When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

A. RADIUS
B. Remote Access and RADIUS
C. AD Query
D. AD Query and Browser-based Authentication

Answer: D

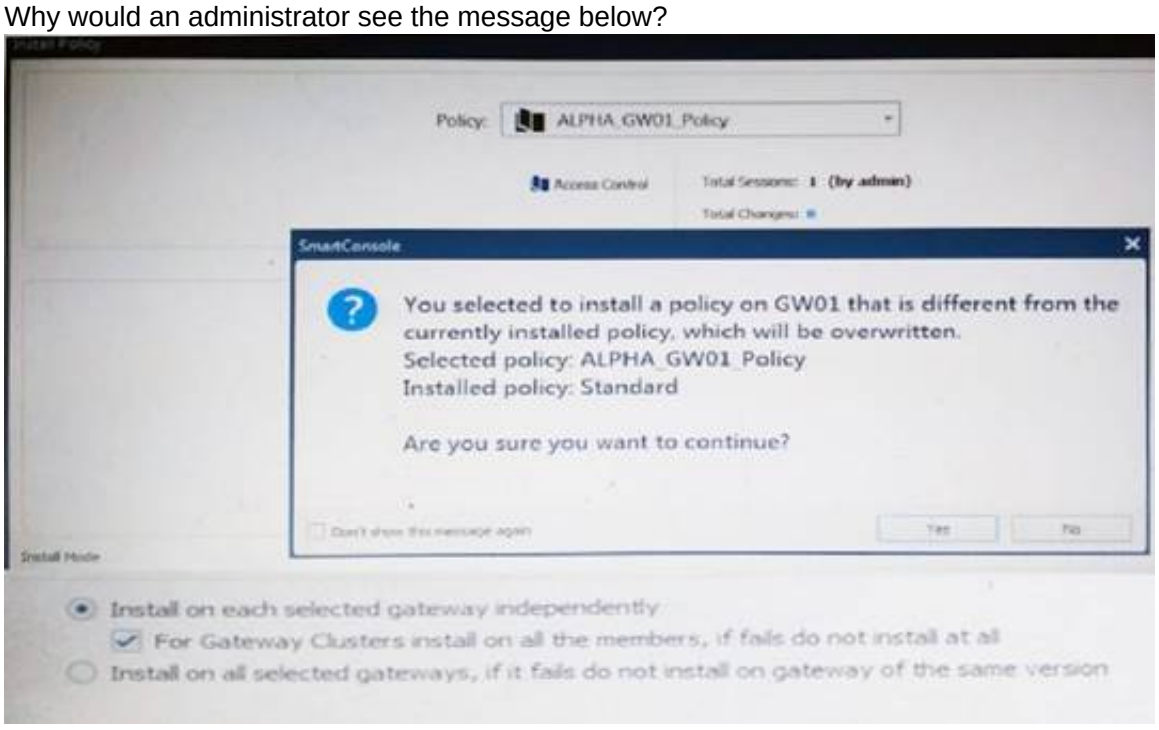
Explanation:
Identity Awareness gets identities from these acquisition sources:
AD Query
Browser-Based Authentication
Endpoint Identity Agent
Terminal Servers Identity Agent
Remote Access

NEW QUESTION 179
- (Exam Topic 2)
Where do we need to reset the SIC on a gateway object?

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

Answer: A

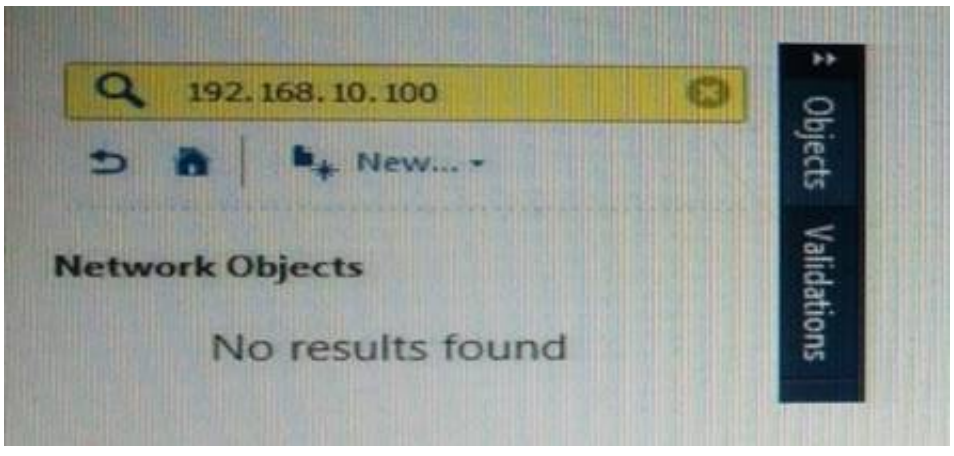
NEW QUESTION 181
- (Exam Topic 2)
Why would an administrator see the message below?



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

Answer: B

NEW QUESTION 182
- (Exam Topic 2)
What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.



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

Answer: B

NEW QUESTION 186
- (Exam Topic 2)
Which of the following is NOT an advantage to using multiple LDAP servers?

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

Answer: B

NEW QUESTION 189
- (Exam Topic 2)
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 191
- (Exam Topic 2)
Which of the following is NOT a VPN routing option available in a star community?

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

Answer: A

Explanation:
SmartConsole
For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:
On the Star Communitywindow, in the:
Center Gateways section, select the Security Gateway that functions as the "Hub".
Satellite Gateways section, select Security Gateways as the "spokes", or satellites.
On the VPN Routing page, Enable VPN routing for satellites section, select one of these options:
To center and to other Satellites through center - This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security Gateway with a static IP address.
To center, or through the center to other satellites, to internet and other VPN targets - This allows connectivity between the Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.
Create an appropriate Access Control Policy rule.
NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.
The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.

NEW QUESTION 193
- (Exam Topic 2)
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, gateway policy permits access only from 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 198
- (Exam Topic 2)
Which of these components does NOT require a Security Gateway R77 license?

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

Answer: C

NEW QUESTION 203
- (Exam Topic 2)
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

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

Answer: D

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

NEW QUESTION 208
- (Exam Topic 2)
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 210
- (Exam Topic 2)
Fill in the blanks: A Check Point software license consists of a _____ and _____.

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

Answer: B

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

NEW QUESTION 211
- (Exam Topic 2)
If there is an Accept Implied Policy set to “First”, what is the reason Jorge cannot see any logs?

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

Answer: A

Explanation:
Implied Rules are configured only on Global Properties.

NEW QUESTION 214
- (Exam Topic 2)
Fill in the blanks: A security Policy is created in _____, stored in the _____, and Distributed to the various _____.

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

Answer: C

NEW QUESTION 218
- (Exam Topic 2)
Which directory holds the SmartLog index files by default?

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

Answer: A

NEW QUESTION 223
- (Exam Topic 2)
Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

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

Answer: D

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

NEW QUESTION 228
- (Exam Topic 2)
You installed Security Management Server on a computer using GAiA in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second GAiA computer, which you plan to ship to another Administrator at a MegaCorp hub office. What is the correct order for pushing SIC certificates to the Gateway before shipping it?
1. Run cpconfig on the Gateway, select Secure Internal Communication, enter the activation key, and reconfirm.
2. Initialize Internal Certificate Authority (ICA) on the Security Management Server.
3. Configure the Gateway object with the host name and IP addresses for the remote site.
4. Click the Communication button in the Gateway object's General screen, enter the activation key, and click Initialize and OK.
5. Install the Security Policy.

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

Answer: B

NEW QUESTION 232
- (Exam Topic 2)
Choose what BEST describes users on Gaia Platform.

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

Answer: B

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

NEW QUESTION 235
- (Exam Topic 2)
Which feature in R77 permits blocking specific IP addresses for a specified time period?

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

Answer: A

NEW QUESTION 240
- (Exam Topic 2)
What is the default shell of Gaia CLI?

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

Answer: B

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

NEW QUESTION 245
- (Exam Topic 2)
Which policy type is used to enforce bandwidth and traffic control rules?

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

Answer: C

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

NEW QUESTION 250
- (Exam Topic 2)
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 254
- (Exam Topic 2)
Anti-Spoofing is typically set up on which object type?

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

Answer: A

NEW QUESTION 255
- (Exam Topic 2)
What is the default method for destination NAT?

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

Answer: D

NEW QUESTION 256
- (Exam Topic 2)
Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____.

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

Answer: B

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

NEW QUESTION 258
- (Exam Topic 2)
Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?

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

Answer: C

NEW QUESTION 260
- (Exam Topic 2)
What happens if the identity of a user is known?

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

Answer: D

NEW QUESTION 265
- (Exam Topic 2)
What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

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

Answer: D

NEW QUESTION 269
- (Exam Topic 2)
Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

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

Answer: B

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

NEW QUESTION 273

- (Exam Topic 2)
The IT Management team is interested in the new features of the Check Point R80 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80 because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

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

Answer: A

NEW QUESTION 275
- (Exam Topic 2)
The most important part of a site-to-site VPN deployment is the ____.

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

Answer: C

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

NEW QUESTION 276
- (Exam Topic 2)
Look at the following screenshot and select the BEST answer.

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

Answer: A

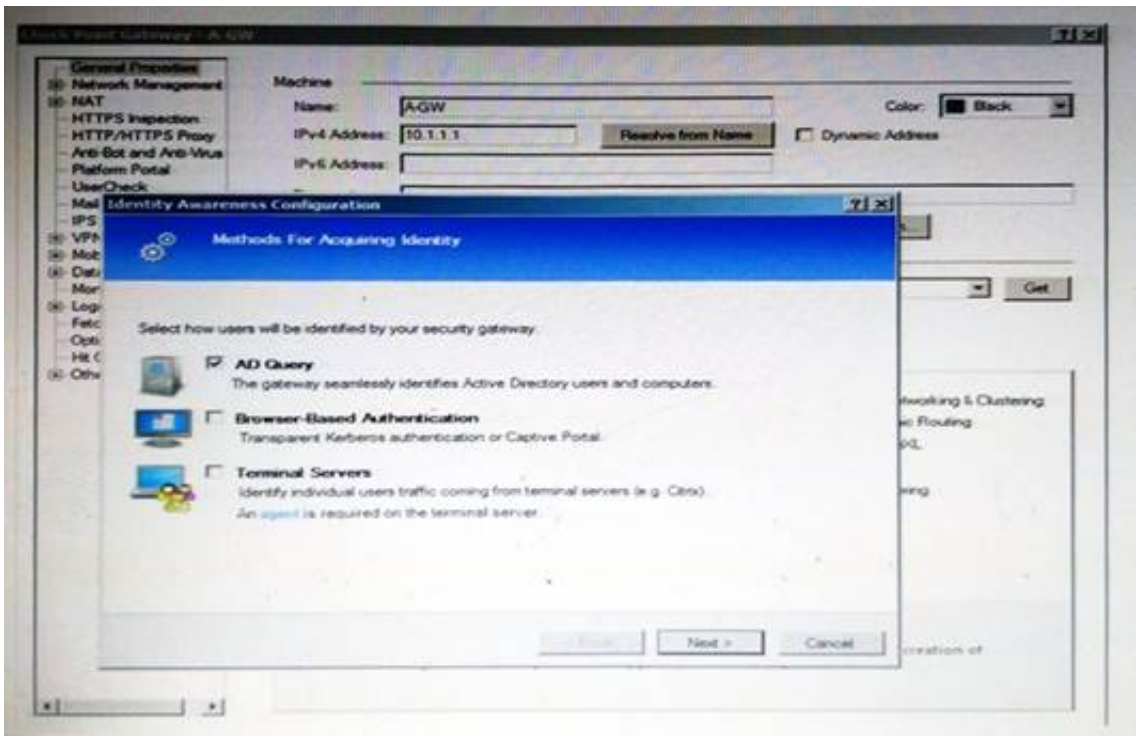
NEW QUESTION 278
- (Exam Topic 2)
Which authentication scheme requires a user to possess a token?

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

Answer: B

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

NEW QUESTION 283
- (Exam Topic 2)
On the following picture an administrator configures Identity Awareness:



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

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

Answer: B

Explanation:
To enable Identity Awareness:
Log in to R80 SmartConsole.
From the Awareness.
Gateway&s
Servers
view, double-click the Security Gateway on which to enable Identity
On the Network Security tab, select Identity Awareness.
The Identity Awareness
Configuration wizard opens.
Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.
AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers
Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.
Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).

NEW QUESTION 284
- (Exam Topic 2)
What port is used for delivering logs from the gateway to the management server?

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

Answer: C

NEW QUESTION 289
- (Exam Topic 2)
You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?

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

Answer: C

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

NEW QUESTION 293
- (Exam Topic 2)
How many users can have read/write access in Gaia at one time?

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

Answer: B

NEW QUESTION 298
- (Exam Topic 2)
Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

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

Answer: A

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

NEW QUESTION 302
- (Exam Topic 2)
R80 Security Management Server can be installed on which of the following operating systems?

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

Answer: A

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

NEW QUESTION 303
- (Exam Topic 2)
The organization's security manager wishes to back up just the Gaia operating system parameters. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries?

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

Answer: B

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

NEW QUESTION 307
- (Exam Topic 3)
Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

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

Answer: B

NEW QUESTION 312
- (Exam Topic 3)
Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?

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

D. Each NIC has one traffic queue that is handled by one CPU

Answer: C

NEW QUESTION 316
- (Exam Topic 3)
What is the mechanism behind Threat Extraction?

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

Answer: D

NEW QUESTION 319
- (Exam Topic 3)
The Firewall kernel is replicated multiple times, therefore:

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

Answer: D

NEW QUESTION 322
- (Exam Topic 3)
What component of R80 Management is used for indexing?

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

Answer: D

NEW QUESTION 323
- (Exam Topic 3)
Which is the correct order of a log flow processed by SmartEvent components:

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

Answer: D

NEW QUESTION 324
- (Exam Topic 3)
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

A. Secure Internal Communication (SIC)
B. Restart Daemons if they fail
C. Transfer messages between Firewall processes
D. Pulls application monitoring status

Answer: D

NEW QUESTION 326
- (Exam Topic 3)
Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.
To make this scenario work, the IT administrator must:
1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
4) Install policy.
Ms McHanry tries to access the resource but is unable. What should she do?

A. Have the security administrator select the Action field of the Firewall Rule “Redirect HTTP connections to an authentication (captive) portal”.
B. Have the security administrator reboot the firewall.
C. Have the security administrator select Any for the Machines tab in the appropriate Access Role.
D. Install the Identity Awareness agent on her iPad.

Answer: A

NEW QUESTION 329
- (Exam Topic 3)
Your boss wants you to closely monitor an employee suspected of transferring company secrets to the competition. The IT department discovered the suspect installed a WinSCP client in order to use encrypted
communication. Which of the following methods is BEST to accomplish this task?

A. Use SmartView Tracker to follow his actions by filtering log entries that feature the WinSCP destination por
B. Then, export the corresponding entries to a separate log file for documentation.
C. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential targets and suspicious protocol
D. Apply the alert action or customized messaging.
E. Watch his IP in SmartView Monitor by setting an alert action to any packet that matches your Rule Base and his IP address for inbound and outbound traffic.
F. Send the suspect an email with a keylogging Trojan attached, to get direct information about his wrongdoings.

Answer: A

NEW QUESTION 334
- (Exam Topic 3)
Which of the below is the MOST correct process to reset SIC from SmartDashboard?

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

Answer: B

NEW QUESTION 335
- (Exam Topic 3)
An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).
Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.
If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.
Which of the following is the BEST Explanation: for this behavior?

A. The setting Log does not capture this level of detail for GR
B. Set the rule tracking action to Audit since certain types of traffic can only be tracked this way.
C. The log unification process is using a LUUID (Log Unification Unique Identification) that has become 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 339
- (Exam Topic 3)
Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

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

Answer: C

NEW QUESTION 341
- (Exam Topic 3)
Check Point APIs allow system engineers and developers to make changes to their organization’s security policy with CLI tools and Web Services for all of the following except:

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

Answer: A

NEW QUESTION 346
- (Exam Topic 3)

To fully enable Dynamic Dispatcher on a Security Gateway:

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

Answer: A

NEW QUESTION 351
- (Exam Topic 3)
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 355
- (Exam Topic 3)
Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

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

Answer: B

NEW QUESTION 358
- (Exam Topic 3)
You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

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

Answer: D

NEW QUESTION 361
- (Exam Topic 3)
Review the rules. Assume domain UDP is enabled in the implied rules.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http, ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets

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 363
- (Exam Topic 3)
A digital signature:

A. Guarantees the authenticity and integrity of a message.

B. Automatically exchanges shared keys.
C. Decrypts data to its original form.
D. Provides a secure key exchange mechanism over the Internet.

Answer: A

NEW QUESTION 366
- (Exam Topic 3)
You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

A. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0.fws configuration file.
B. Select Block intruder from the Tools menu in SmartView Tracker.
C. Create a Suspicious Activity Rule in Smart Monitor.
D. Add a temporary rule using SmartDashboard and select hide rule.

Answer: C

NEW QUESTION 368
- (Exam Topic 3)
Which of the following uses the same key to decrypt as it does to encrypt?

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

Answer: D

NEW QUESTION 371
- (Exam Topic 3)
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

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

Answer: A

NEW QUESTION 374
- (Exam Topic 3)
Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?

A. Dynamic ID
B. RADIUS
C. Username and Password
D. Certificate

Answer: A

NEW QUESTION 379
- (Exam Topic 3)
On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

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

Answer: B

NEW QUESTION 382
- (Exam Topic 3)
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 386
- (Exam Topic 3)

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 387
- (Exam Topic 3)
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 388
- (Exam Topic 3)
There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?

A. Using Web Services
B. Using Mgmt_cli tool
C. Using CLISH
D. Using SmartConsole GUI console

Answer: C

NEW QUESTION 393
- (Exam Topic 3)
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100
Web Filtering Categories	☐	100
Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
Special properties	☐	100

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

Answer: B

NEW QUESTION 397
- (Exam Topic 3)
Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

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

Answer: D

NEW QUESTION 399
- (Exam Topic 3)
Which one of the following is true about Threat Extraction?

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

Answer: B

NEW QUESTION 403
- (Exam Topic 3)
Where would an administrator enable Implied Rules logging?

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

Answer: B

NEW QUESTION 406
- (Exam Topic 3)
You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After a while, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

A. Run fwm dbexport -1 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 407
- (Exam Topic 3)
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 409
- (Exam Topic 3)
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 412
- (Exam Topic 3)
What port is used for communication to the User Center with SmartUpdate?

A. CPMI 200
B. TCP 8080
C. HTTP 80
D. HTTPS 443

Answer: D

NEW QUESTION 416
- (Exam Topic 3)
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 421
- (Exam Topic 3)
All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

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

Answer: B

NEW QUESTION 423
- (Exam Topic 3)
What are types of Check Point APIs available currently as part of R80.10 code?

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

Answer: B

NEW QUESTION 425
- (Exam Topic 3)
Which of these attributes would be critical for a site-to-site VPN?

A. Scalability to accommodate user groups
B. Centralized management
C. Strong authentication
D. Strong data encryption

Answer: D

NEW QUESTION 429
- (Exam Topic 3)
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 430
- (Exam Topic 3)
What happens when you run the command: fw sam -J src [Source IP Address]?

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

Answer: A

NEW QUESTION 434
- (Exam Topic 3)
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 435
- (Exam Topic 3)
You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

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

Answer: A

NEW QUESTION 436

- (Exam Topic 3)
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

NEW QUESTION 441
- (Exam Topic 4)
How are the backups stored in Chock Point appliances?

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

Answer: D

NEW QUESTION 442
- (Exam Topic 4)
R80.10 management server can manage gateways with which versions installed?

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

Answer: B

NEW QUESTION 444
- (Exam Topic 4)
Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

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

Answer: D

NEW QUESTION 449
- (Exam Topic 4)
What is a reason for manual creation of a NAT rule?

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

Answer: D

NEW QUESTION 451
- (Exam Topic 4)
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

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

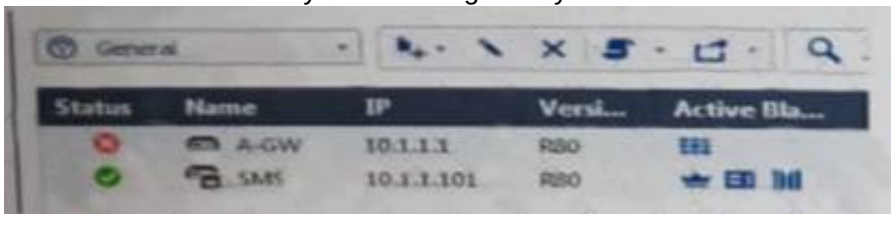
Answer: A

NEW QUESTION 454
- (Exam Topic 4)
What needs to be configured if the NAT property ‘Translate destination on client side’ is not enabled in Global properties?

A. A host route to route to the destination IP
B. Use the file local.arp to add the ARP entries for NAT to work
C. Nothing, the Gateway takes care of all details necessary
D. Enabling 'Allow bi-directional NAT' for NAT to work correctly

Answer: C

NEW QUESTION 458
- (Exam Topic 4)
What does it mean if Deyra sees the gateway status



Choose the BEST answer.

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

Answer: A

NEW QUESTION 463
- (Exam Topic 4)
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

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

Answer: C

NEW QUESTION 466
- (Exam Topic 4)
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

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

Answer: B

NEW QUESTION 469
- (Exam Topic 4)
The _____ software blade package uses CPU-level and OS-level sandboxing in order to delect and block malware.

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

Answer: B

NEW QUESTION 472
- (Exam Topic 4)
Fill in the blank: Authentication rules are defined for ____ .

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

Answer: A

NEW QUESTION 476
- (Exam Topic 4)
You want to store the GAiA configuration in a file for later reference. What command should you use?

A. write mem <filename>
B. show config -f <filename>

C. save config -o <filename>
D. save configuration <filename>

Answer: D

NEW QUESTION 481
- (Exam Topic 4)
The SmartEvent R80 Web application for real-time event monitoring is called:

A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView

Answer: B

NEW QUESTION 484
- (Exam Topic 4)
Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

What is the possible Explanation: for this?

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

Answer: B

NEW QUESTION 489
- (Exam Topic 4)
If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

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

Answer: A

NEW QUESTION 493
- (Exam Topic 4)
Fill in the blank: In Security Gateways R75 and above, SIC uses _____ for encryption.

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

Answer: A

NEW QUESTION 494
- (Exam Topic 4)
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 499

- (Exam Topic 4)
Can multiple administrators connect to a Security Management Server at the same time?

A. No, only one can be connected
B. Yes, all administrators can modify a network object at the same time
C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
D. Yes, but only one has the right to write

Answer: C

NEW QUESTION 504
- (Exam Topic 4)
Which of the following is NOT an option to calculate the traffic direction?

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

Answer: D

NEW QUESTION 507
- (Exam Topic 4)
Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Answer: B

NEW QUESTION 512
- (Exam Topic 4)
Using ClusterXL, what statement is true about the Sticky Decision Function?

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

Answer: A

NEW QUESTION 516
- (Exam Topic 4)
How would you determine the software version from the CLI?

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

Answer: A

NEW QUESTION 518
- (Exam Topic 4)
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

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

Answer: B

NEW QUESTION 519
- (Exam Topic 4)
What is the purpose of the Clean-up Rule?

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

Answer: A

NEW QUESTION 523
- (Exam Topic 4)
Which Threat Prevention Profile is not included by default in R80 Management?

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

Answer: D

NEW QUESTION 524
- (Exam Topic 4)
What is true about the IPS-Blade?

A. in R80, IPS is managed by the Threat Prevention Policy
B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
C. in R80, IPS Exceptions cannot be attached to “all rules”
D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 527
- (Exam Topic 4)
What is the best sync method in the ClusterXL deployment?

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

Answer: B

NEW QUESTION 528
- (Exam Topic 4)
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 532
- (Exam Topic 4)
Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 535
- (Exam Topic 4)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 539
- (Exam Topic 4)
Which deployment adds a Security Gateway to an existing environment without changing IP routing?

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

Answer:

B

NEW QUESTION 540
- (Exam Topic 4)
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 545
- (Exam Topic 4)
Under which file is the proxy arp configuration stored?

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

Answer: D

NEW QUESTION 548
- (Exam Topic 4)
When using Monitored circuit VRRP, what is a priority delta?

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

Answer: C

NEW QUESTION 551
- (Exam Topic 4)
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 553
- (Exam Topic 4)
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

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

Answer: D

NEW QUESTION 557
- (Exam Topic 4)
Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

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

Answer: D

NEW QUESTION 560
- (Exam Topic 4)
Which repositories are installed on the Security Management Server by SmartUpdate?

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

D. License and Contract and Package Repository

Answer: D

NEW QUESTION 561
- (Exam Topic 4)
What are the three components for Check Point Capsule?

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

Answer: D

NEW QUESTION 563
- (Exam Topic 4)
What is the difference between SSL VPN and IPSec VPN?

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

Answer: D

NEW QUESTION 568
- (Exam Topic 4)
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 569
- (Exam Topic 4)
Which of the following is NOT a method used by Identity Awareness for acquiring identity?

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

Answer: D

NEW QUESTION 571
- (Exam Topic 4)
Choose what BEST describes the reason why querying logs now is very fast.

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

Answer: B

NEW QUESTION 572
- (Exam Topic 4)
True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

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

Answer: B

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

NEW QUESTION 577

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

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

Answer: C

NEW QUESTION 581
- (Exam Topic 4)
After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust
B. The Security Gateway name cannot be changed in command line without re-establishing trust
C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Answer: A

NEW QUESTION 584
- (Exam Topic 4)
Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

A. The firewall topologies
B. NAT Rules
C. The Rule Base
D. The VPN Domains

Answer: C

NEW QUESTION 585
- (Exam Topic 4)
Which GUI tool can be used to view and apply Check Point licenses?

A. cpconfig
B. Management Command Line
C. SmartConsole
D. SmartUpdate

Answer: D

Explanation:
SmartUpdate GUI is the recommended way of managing licenses. References:

NEW QUESTION 588
- (Exam Topic 4)
What is the main difference between Threat Extraction and Threat Emulation?

A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
B. Threat Extraction always delivers a file and takes less than a second to complete
C. Threat Emulation never delivers a file that takes less than a second to complete
D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Answer: B

NEW QUESTION 590
- (Exam Topic 4)
You want to verify if there are unsaved changes in GAiA that will be lost with a reboot. What command can be used?

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

Answer: D

NEW QUESTION 594
- (Exam Topic 4)
In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

A. 3rd Party integration of CLI and API for Gateways prior to R80.
B. A complete CLI and API interface using SSH and custom CPCode integration.
C. 3rd Party integration of CLI and API for Management prior to R80.
D. A complete CLI and API interface for Management with 3rd Party integration.

Answer: B

NEW QUESTION 596
- (Exam Topic 4)
Which two Identity Awareness commands are used to support identity sharing?

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

Answer: A

NEW QUESTION 598
- (Exam Topic 4)
Which statement is NOT TRUE about Delta synchronization?

A. Using UDP Multicast or Broadcast on port 8161
B. Using UDP Multicast or Broadcast on port 8116
C. Quicker than Full sync
D. Transfers changes in the Kernel tables between cluster members

Answer: A

NEW QUESTION 600
- (Exam Topic 4)
Which of the following is the most secure means of authentication?

A. Password
B. Certificate
C. Token
D. Pre-shared secret

Answer: B

NEW QUESTION 605
- (Exam Topic 4)
Using R80 Smart Console, what does a “pencil icon” in a rule mean?

A. I have changed this rule
B. Someone else has changed this rule
C. This rule is managed by check point’s SOC
D. This rule can’t be changed as it’s an implied rule

Answer: A

NEW QUESTION 610
- (Exam Topic 4)
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

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

Answer: D

NEW QUESTION 614
- (Exam Topic 4)
Session unique identifiers are passed to the web api using which http header option?

A. X-chkp-sid
B. Accept-Charset
C. Proxy-Authorization
D. Application

Answer: C

NEW QUESTION 618
- (Exam Topic 4)
How Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VP
B. Capsule Workspace provides a Desktop with usable applications

C. Capsule Workspace can provide access to any application
D. Capsule Connect provides Business data isolation
E. Capsule Connect does not require an installed application at client

Answer: A

NEW QUESTION 619
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

156-215.80 Practice Exam Features:

* 156-215.80 Questions and Answers Updated Frequently

* 156-215.80 Practice Questions Verified by Expert Senior Certified Staff

* 156-215.80 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 156-215.80 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year