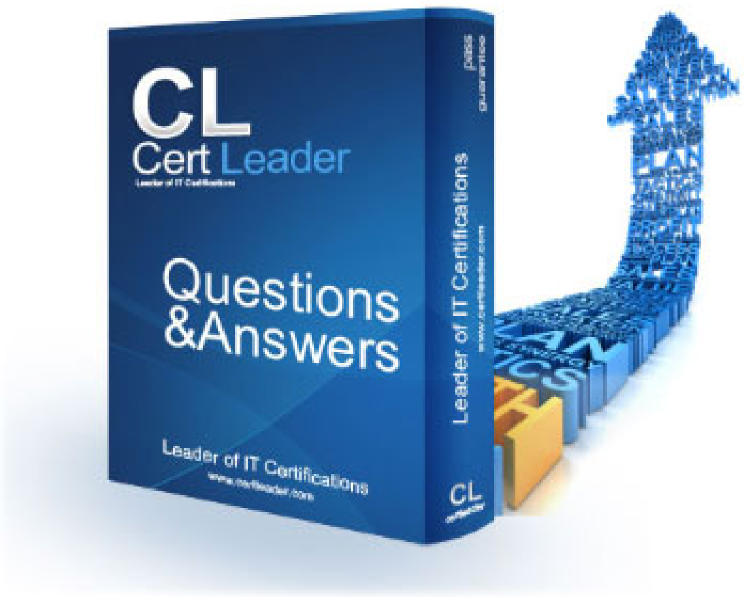
156-215.80 Dumps

Check Point Certified Security Administrator

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

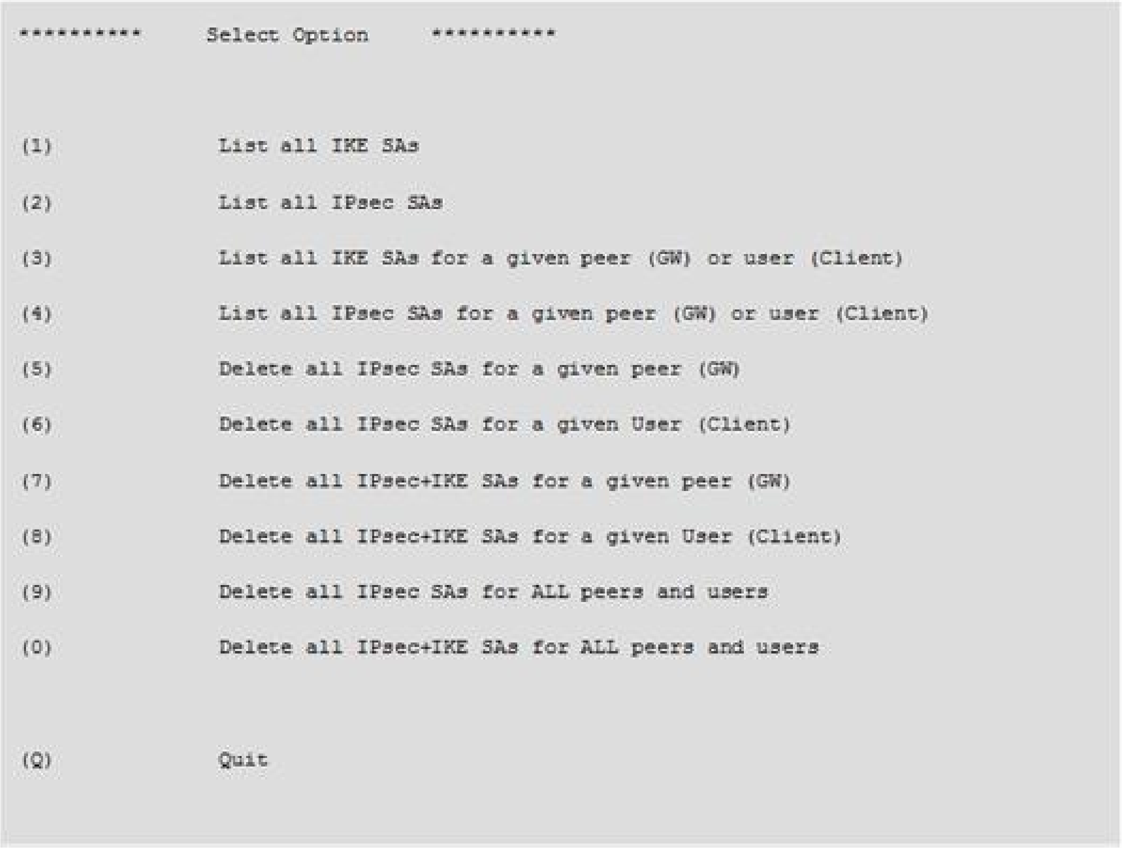


NEW QUESTION 1
- (Exam Topic 1)
Which of the following commands can be used to remove site-to-site IPSEC Security Associations (SA)?

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 statements is TRUE about R80 management plug-ins?

A. The plug-in is a package installed on the Security Gateway.
B. Installing a management plug-in requires a Snapshot, just like any upgrade process.
C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Answer: C

NEW QUESTION 3
- (Exam Topic 1)
Which of the following is NOT a SecureXL traffic flow?

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

Answer: C

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

NEW QUESTION 4
- (Exam Topic 1)
While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows

domain?

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

Answer: B

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

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
Which default user has full read/write access?

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

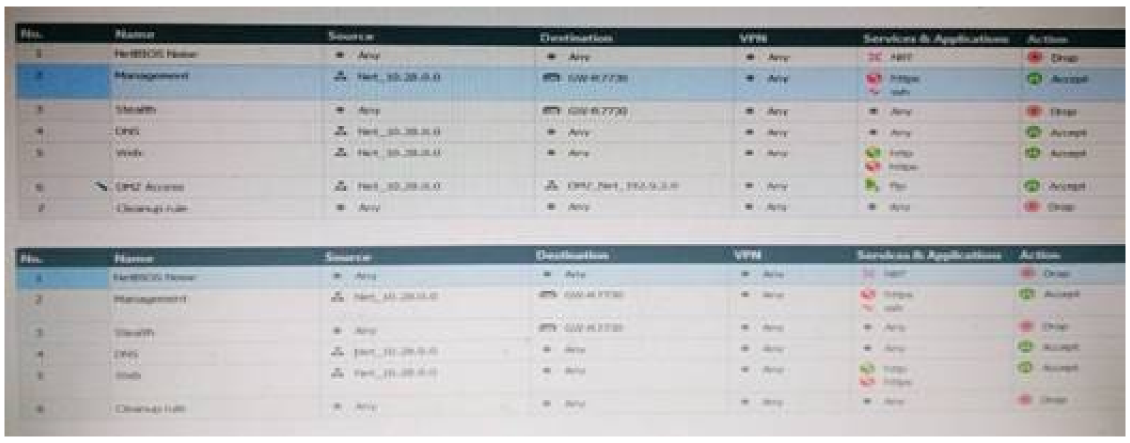
Answer: C

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
Two administrators Dave and Jon both manage R80 Management as administrators for ABC Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it his in his SmartConsole view?



No.	Name	Source	Destination	VPN	Services & Applications	Action
1	NetBIOS Noise	Any	Any	Any	NBT	Drop
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept
3	Stealth	Any	GW-R7730	Any	Any	Drop
4	DNS	Net_10.28.0.0	Any	Any	Any	Accept
5	Web	Net_10.28.0.0	Any	Any	http https	Accept
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.9.3.0	Any	ftp	Accept
7	Cleanup rule	Any	Any	Any	Any	Drop

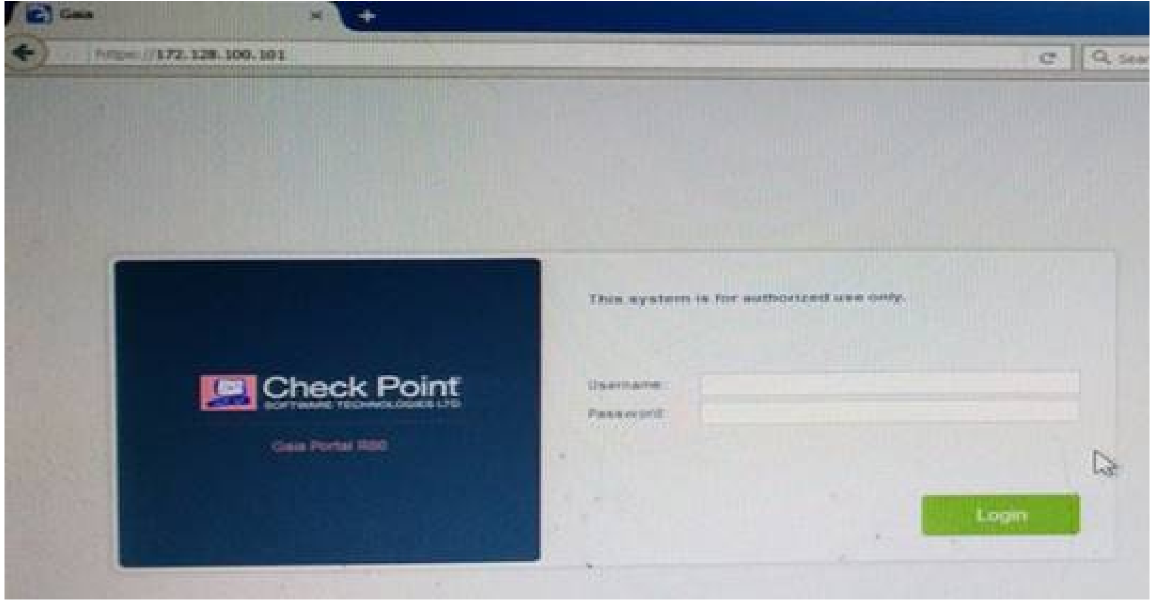
No.	Name	Source	Destination	VPN	Services & Applications	Action
1	NetBIOS Noise	Any	Any	Any	NBT	Drop
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept
3	Stealth	Any	GW-R7730	Any	Any	Drop
4	DNS	Net_10.28.0.0	Any	Any	Any	Accept
5	Web	Net_10.28.0.0	Any	Any	http https	Accept
6	Cleanup rule	Any	Any	Any	Any	Drop

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

Answer: D

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

NEW QUESTION 9
- (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?



This system is for authorized use only.

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 10
- (Exam Topic 1)
Fill in the blank: The R80 utility fw monitor is used to troubleshoot _______

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

Answer: C

Explanation:

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

NEW QUESTION 10
- (Exam Topic 1)
When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored

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

Answer: C

Explanation:
SmartUpdate installs two repositories on the Security Management server:
License & Contract Repository, which is stored on all platforms in the directory $FWDIR\conf\.
Package Repository, which is stored:
on Windows machines in C:\SUroot.
on UNIX machines in /var/suroot.
The Package Repository requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the Package Repository.

NEW QUESTION 14
- (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.

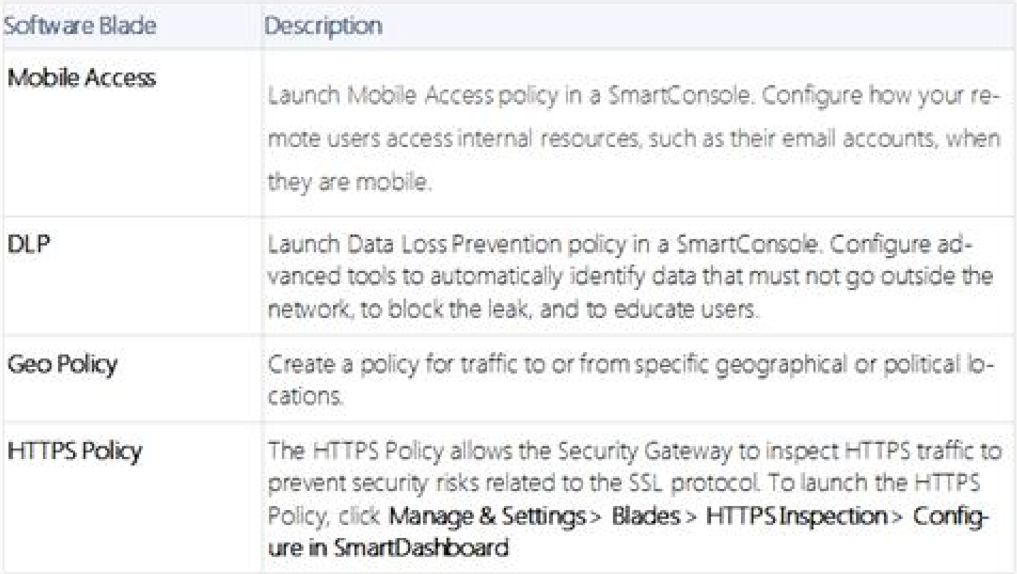
Answer: B

NEW QUESTION 17
- (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 22
- (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 25
- (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 27
- (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.

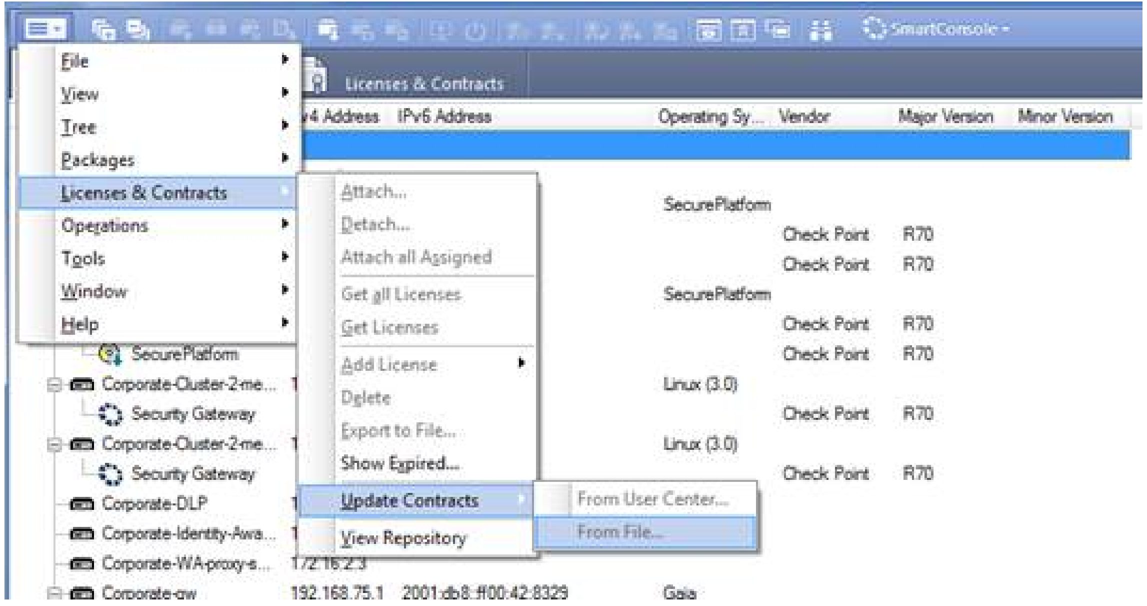
Answer: B

NEW QUESTION 29
- (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 32
- (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 35
- (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 36
- (Exam Topic 1)
Fill in the blank: Gaia can be configured using the _____ or _____.

A. Gaia; command line interface
B. WebUI; Gaia Interface
C. Command line interface; WebUI
D. Gaia Interface; GaiaUI

Answer: C

Explanation:
Configuring Gaia for the First Time In This Section:
Running the First Time Configuration Wizard in WebUI Running the First Time Configuration Wizard in CLI
After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

NEW QUESTION 40
- (Exam Topic 1)
What is the order of NAT priorities?

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

Answer: A

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

NEW QUESTION 44
- (Exam Topic 1)
Which Check Point feature enables application scanning and the detection?

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

Answer: B

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

NEW QUESTION 48
- (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 51
- (Exam Topic 1)
If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

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

Answer: A

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

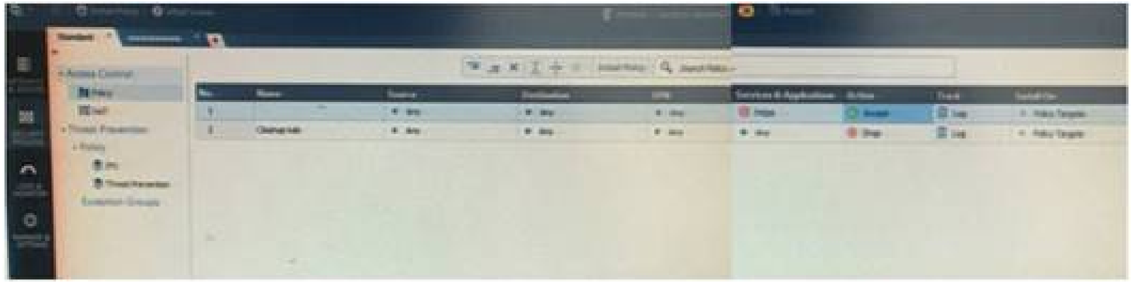
NEW QUESTION 52
- (Exam Topic 1)
In R80 spoofing is defined as a method of:

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

Answer: D

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

NEW QUESTION 57
- (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 61
- (Exam Topic 1)
Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

A. Central

B. Corporate
C. Formal
D. Local

Answer: D

NEW QUESTION 63
- (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 68
- (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 69
- (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 74
- (Exam Topic 1)
Which policy type has its own Exceptions section?

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

Answer: A

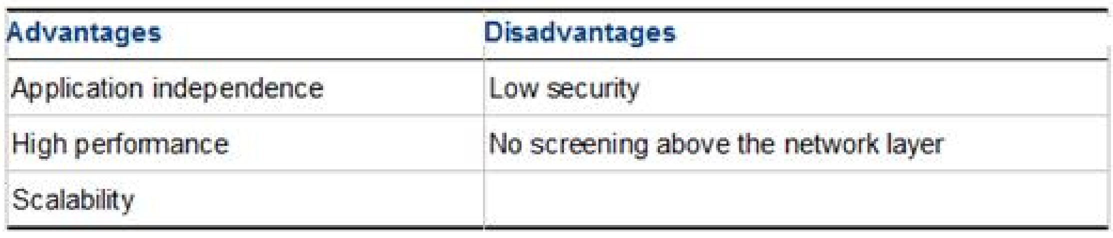
Explanation:
The Exceptions Groups pane lets you define exception groups. When necessary, you can create exception groups to use in the Rule Base. An exception group contains one or more defined exceptions. This option facilitates ease-of-use so you do not have to manually define exceptions in multiple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

NEW QUESTION 76
- (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 79
- (Exam Topic 1)
Fill in the blank: Each cluster has _____ interfaces.

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

Answer: C

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

NEW QUESTION 84
- (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 85
- (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 86
- (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 88
- (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 92
- (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 97
- (Exam Topic 1)
Which Threat Prevention Software Blade provides comprehensive against malicious and unwanted network traffic, focusing on application and server vulnerabilities?

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

Answer: B

Explanation:
The IPS Software Blade provides a complete Intrusion Prevention System security solution, providing comprehensive network protection against malicious and unwanted network traffic, including:
 Malware attacks
 Dos and DDoS attacks
 Application and server vulnerabilities
 Insider threats
 Unwanted application traffic, including IM and P2P

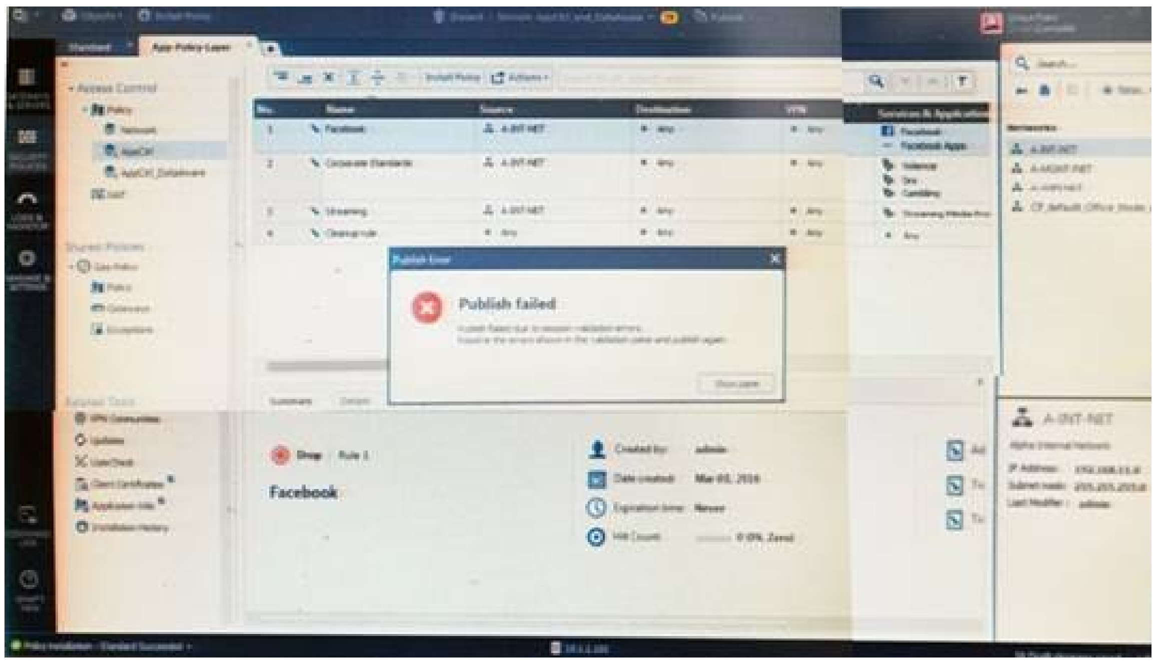
NEW QUESTION 100
- (Exam Topic 1)
Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?

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 103
- (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?



Publish Error

Publish failed

Show pane

Facebook

Created by: admin

Date created: Mar 03, 2016

Expiration time: Never

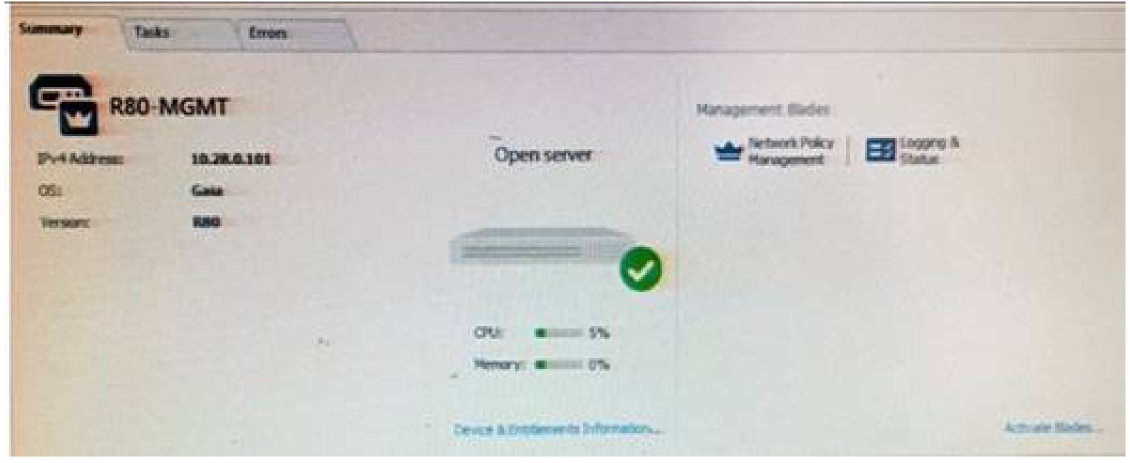
Hit Count: 0 0% Zero

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 108
- (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'?



R80-MGMT

IPv4 Address: 10.28.0.101

OS: Gaia

Version: R80

Open server

CPU: 5%

Memory: 0%

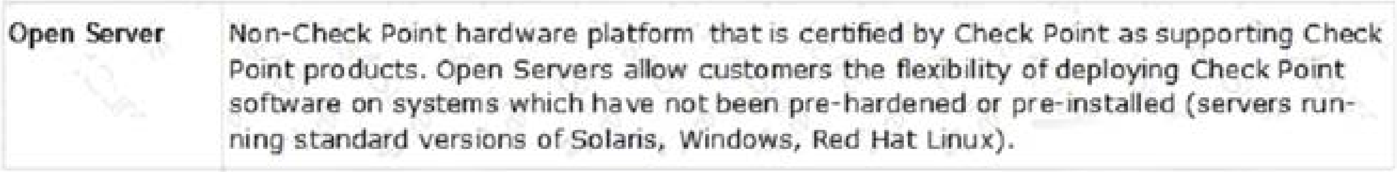
Management Blades

Network Policy Management
Logging & Status
Device & Entitlements Information...
Activate Blades...

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 113
- (Exam Topic 2)
Mesh and Star are two types of VPN topologies. Which statement below is TRUE about these types of communities?

A. A star community requires Check Point gateways, as it is a Check Point proprietary technology.
B. In a star community, satellite gateways cannot communicate with each other.
C. In a mesh community, member gateways cannot communicate directly with each other.
D. In a mesh community, all members can create a tunnel with any other member.

Answer: D

NEW QUESTION 116

- (Exam Topic 2)
Which Check Point software blade provides protection from zero-day and undiscovered threats?

A. Firewall
B. Threat Emulation
C. Application Control
D. Threat Extraction

Answer: D

Explanation:
SandBlast Threat Emulation
As part of the Next Generation Threat Extraction software bundle (NGTX), the SandBlast Threat Emulation capability prevents infections from undiscovered exploits zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network.

NEW QUESTION 119
- (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 120
- (Exam Topic 2)
Which of the following is NOT defined by an Access Role object?

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

Answer: D

NEW QUESTION 121
- (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 125
- (Exam Topic 2)
You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how many often the particular rules match. Where can you see it? Give the BEST answer.

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

Answer: C

NEW QUESTION 128
- (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 130
- (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

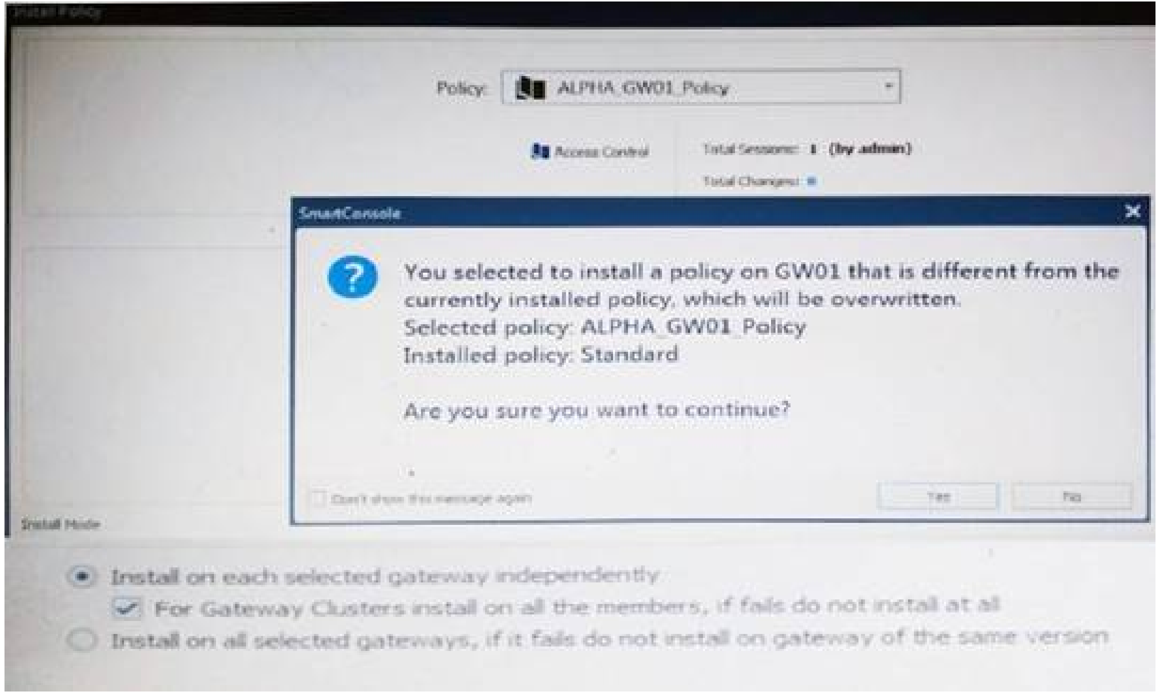
NEW QUESTION 134
- (Exam Topic 2)
Which of the following is NOT an alert option?

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

Answer: B

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

NEW QUESTION 137
- (Exam Topic 2)
Why would an administrator see the message below?



Policy: ALPHA_GW01_Policy

Total Sessions: 1 (by admin)
Total Changes:

SmartConsole

You selected to install a policy on GW01 that is different from the currently installed policy, which will be overwritten.
Selected policy: ALPHA_GW01_Policy
Installed policy: Standard

Are you sure you want to continue?

□ Don't show this message again

Install Mode

● Install on each selected gateway independently
☑ For Gateway Clusters install on all the members, if fails do not install at all
○ Install on all selected gateways, if it fails do not install on gateway of the same version

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

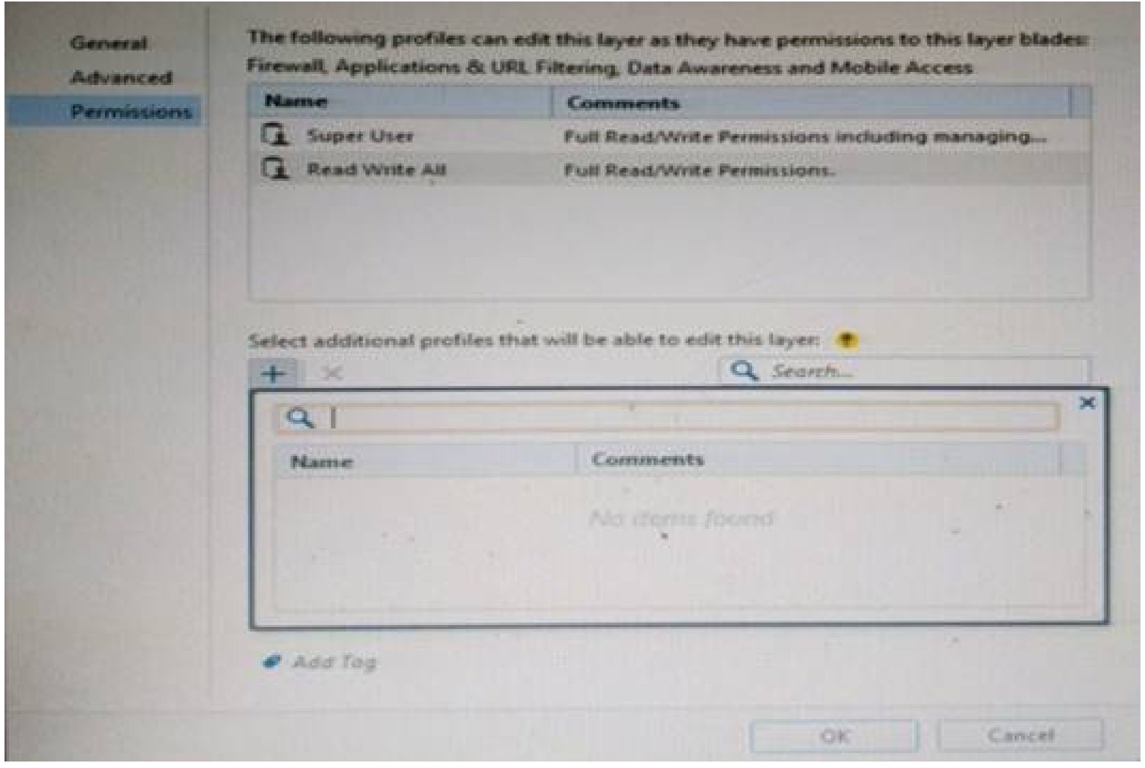
NEW QUESTION 138
- (Exam Topic 2)
Which of the following is NOT a VPN routing option available in a star community?

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

Answer: A

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

NEW QUESTION 139
- (Exam Topic 2)
You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the “Select additional profile that will be able edit this layer” you do not see anything. What is the most likely cause of this problem? Select the BEST answer.



The following profiles can edit this layer as they have permissions to this layer blades: Firewall, Applications & URL Filtering, Data Awareness and Mobile Access

Name	Comments
Super User	Full Read/Write Permissions including managing...
Read Write All	Full Read/Write Permissions.

Select additional profiles that will be able to edit this layer:

Name	Comments
	No items found

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

Answer: B

NEW QUESTION 142
- (Exam Topic 2)
Which of the following is TRUE about the Check Point Host object?

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

Answer: A

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

NEW QUESTION 145
- (Exam Topic 2)
What action can be performed from SmartUpdate R77?

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

Answer: C

NEW QUESTION 148
- (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 153
- (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 156
- (Exam Topic 2)
Fill in the blanks: A High Availability deployment is referred to as a ____ cluster and a Load Sharing deployment is referred to as a _____ cluster.

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

Answer: D

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

NEW QUESTION 161
- (Exam Topic 2)
MyCorp has the following NAT rules. You need to disable the NAT function when Alpha-internal networks try to reach the Google DNS (8.8.8.8) server.
What can you do in this case?

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

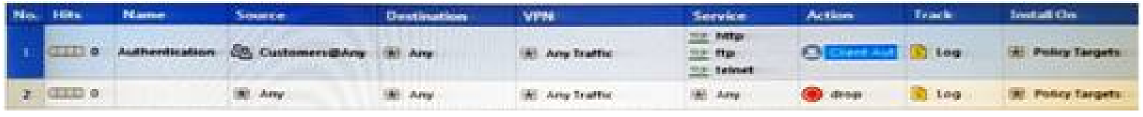
Answer: D

NEW QUESTION 164
- (Exam Topic 2)
Which directory holds the SmartLog index files by default?

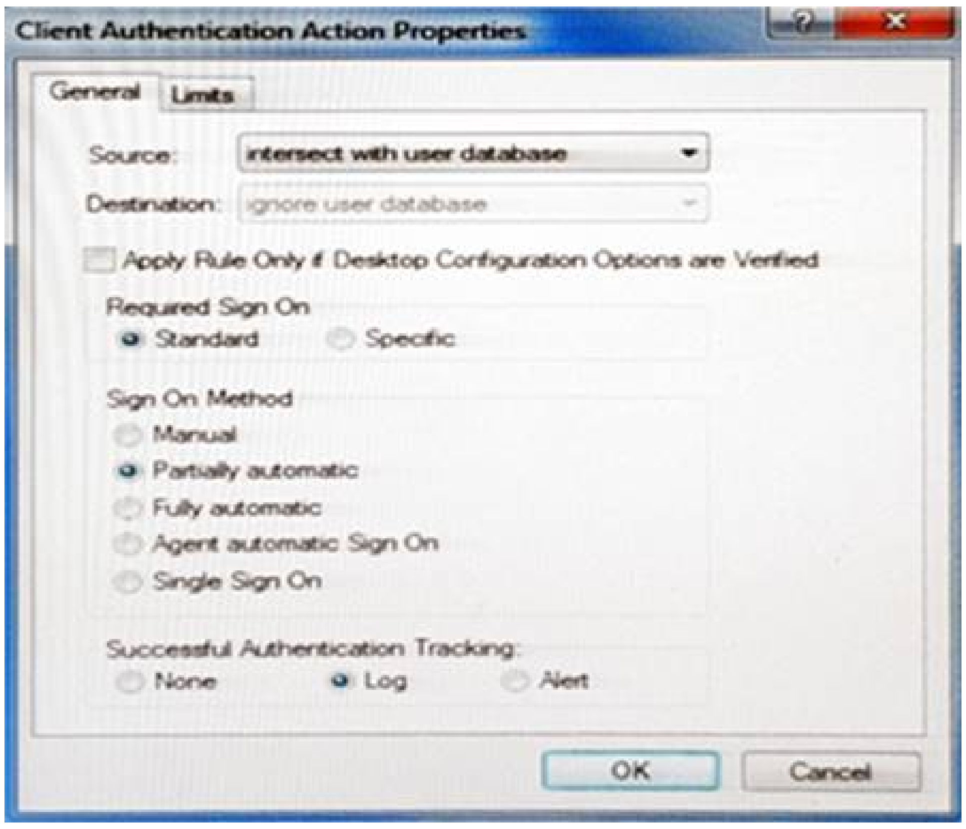
A. $SMARTLOGDIR/data
B. $SMARTLOG/dir
C. $FWDIR/smartlog
D. $FWDIR/log

Answer: A

NEW QUESTION 165
- (Exam Topic 2)
Study the Rule base and Client Authentication Action properties screen.



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp telnet	Client Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	drop	Log	Policy Targets



Client Authentication Action Properties

General | Limits

Source: intersect with user database

Destination: ignore user database

□ Apply Rule Only if Desktop Configuration Options are Verified

Required Sign On
● Standard ○ Specific

Sign On Method
○ Manual
● Partially automatic
○ Fully automatic
○ Agent automatic Sign On
○ Single Sign On

Successful Authentication Tracking:
○ None ● Log ○ Alert

After being authenticated by the Security Gateways, a user starts a HTTP connection to a Web site. What happens when the user tries to FTP to another site using the command line? The:

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

Answer: C

NEW QUESTION 168
- (Exam Topic 2)
After the initial installation the First Time Configuration Wizard should be run. Select the BEST answer.

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

Answer: B

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

NEW QUESTION 169
- (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 170
- (Exam Topic 2)
Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

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

Answer: B

Explanation:

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

NEW QUESTION 171
- (Exam Topic 2)
Choose the SmartLog property that is TRUE.

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

Answer: D

NEW QUESTION 176
- (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 181
- (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 182
- (Exam Topic 2)
There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic in the morning. FW_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW_B became active. After an hour, FW_A's interface issues were resolved and it became operational. When it re-joins the cluster, will it become active automatically?

A. No, since “maintain current active cluster member” option on the cluster object properties is enabled by default
B. No, since “maintain current active cluster member” option is enabled by default on the Global Properties
C. Yes, since “Switch to higher priority cluster member” option on the cluster object properties is enabled by default
D. Yes, since “Switch to higher priority cluster member” option is enabled by default on the Global Properties

Answer: A

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

NEW QUESTION 186
- (Exam Topic 2)
Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

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

Answer: C

NEW QUESTION 189
- (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 192
- (Exam Topic 2)
Fill in the blank: RADIUS Accounting gets _____ data from requests generated by the accounting client

A. Destination
B. Identity
C. Payload
D. Location

Answer: B

Explanation:
How RADIUS Accounting Works with Identity Awareness
RADIUS Accounting gets identity data from RADIUS Accounting Requests generated by the RADIUS accounting client.

NEW QUESTION 193
- (Exam Topic 2)
The Captive Portal tool:

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

Answer: A

NEW QUESTION 196
- (Exam Topic 2)
Which command is used to obtain the configuration lock in Gaia?

A. Lock database override
B. Unlock database override
C. Unlock database lock
D. Lock database user

Answer: A

Explanation:
Obtaining a Configuration Lock
 lock database override
 unlock database

NEW QUESTION 197
- (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 201
- (Exam Topic 2)

Message digests use which of the following?

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

Answer: D

NEW QUESTION 202
- (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 204
- (Exam Topic 2)
Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as ______

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

Answer: B

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

NEW QUESTION 206
- (Exam Topic 2)
You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the
most likely cause?

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

Answer: C

NEW QUESTION 210
- (Exam Topic 2)
Which of the following licenses are considered temporary?

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

Answer: B

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

NEW QUESTION 211
- (Exam Topic 2)
Fill in the blank: Licenses can be added to the License and Contract repository _____.

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

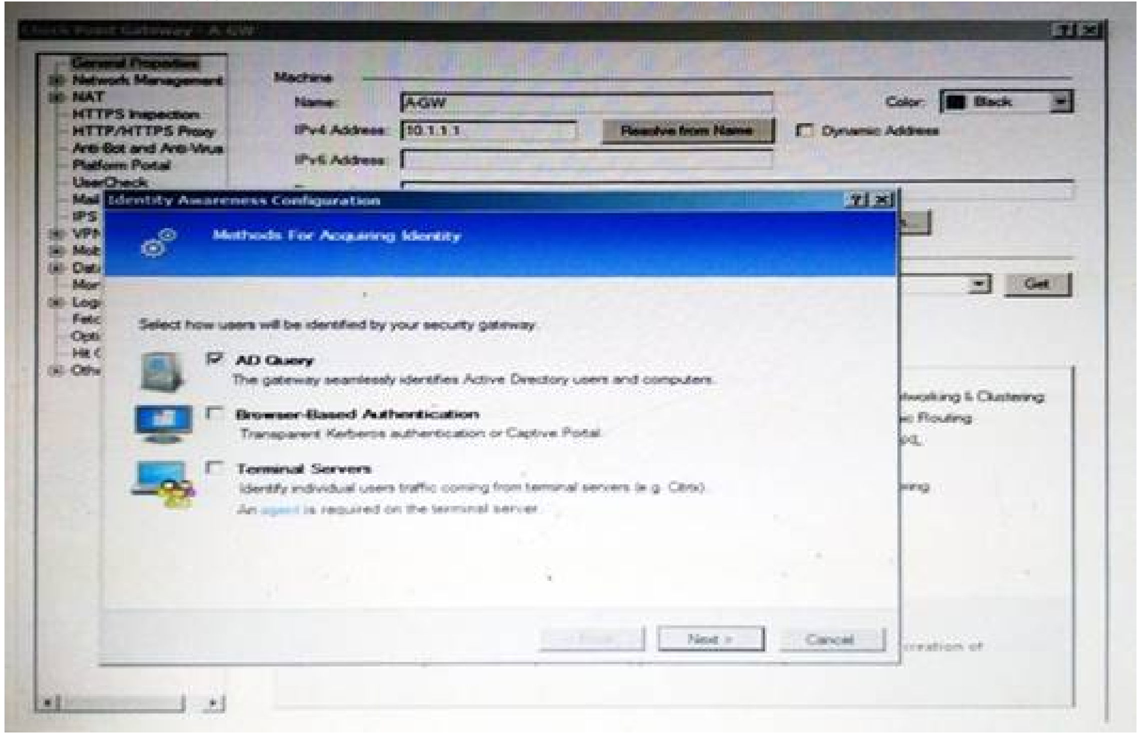
Answer: A

NEW QUESTION 212
- (Exam Topic 2)
When using LDAP as an authentication method for Identity Awareness, the query:

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

Answer: D

NEW QUESTION 213
- (Exam Topic 2)
On the following picture an administrator configures Identity Awareness:



Name: A-GW
IPv4 Address: 10.1.1.1

Select how users will be identified by your security gateway

☑ AD Query
The gateway seamlessly identifies Active Directory users and computers.

☐ Browser-Based Authentication
Transparent Kerberos authentication or Captive Portal

☐ Terminal Servers
Identify individual users traffic coming from terminal servers (e.g. Citrix)
An agent is required on the terminal server

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 214
- (Exam Topic 2)
Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAiA, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

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

Answer: C

NEW QUESTION 215
- (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 218
- (Exam Topic 2)
Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

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

Answer: C

NEW QUESTION 220
- (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 225
- (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 226
- (Exam Topic 3)
In what way are SSL VPN and IPSec VPN different?

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

Answer: D

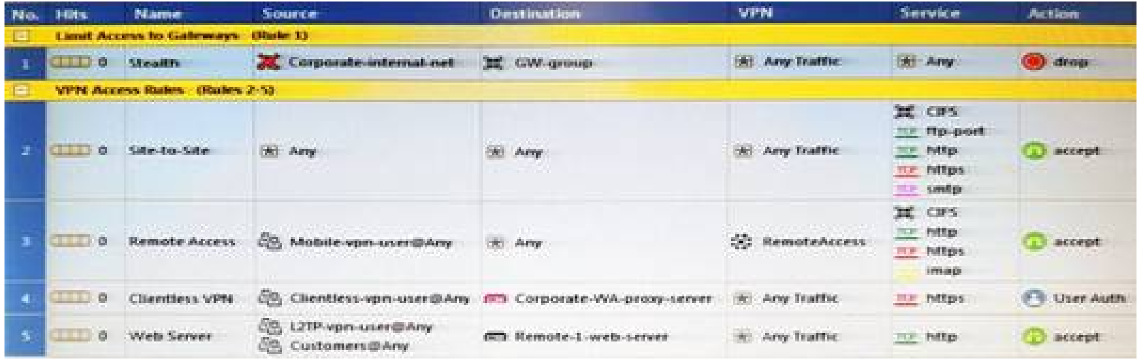
NEW QUESTION 227
- (Exam Topic 3)
What is the mechanism behind Threat Extraction?

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 229
- (Exam Topic 3)

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



No.	Hits	Name	Source	Destination	VPN	Service	Action
	Limit Access to Gateways (Rule 1)						
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
	VPN Access Rules (Rules 2-5)						
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth
5	0	Web Server	L2TP-vpn-user@Any Customers@Any	Remote-1-web-server	Any Traffic	http	accept

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

Answer: B

NEW QUESTION 230
- (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 234
- (Exam Topic 3)
According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

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

Answer: A

NEW QUESTION 235
- (Exam Topic 3)
The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them?

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

Answer: D

NEW QUESTION 237
- (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 239
- (Exam Topic 3)
What is also referred to as Dynamic NAT?

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

Answer: D

NEW QUESTION 240
- (Exam Topic 3)
Which of the following is NOT a valid option when configuring access for Captive Portal?

A. From the Internet
B. Through internal interfaces
C. Through all interfaces
D. According to the Firewall Policy

Answer: A

NEW QUESTION 241
- (Exam Topic 3)
The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

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

Answer: D

NEW QUESTION 243
- (Exam Topic 3)
Which of these statements describes the Check Point ThreatCloud?

A. Blocks or limits usage of web applications
B. Prevents or controls access to web sites based on category
C. Prevents Cloud vulnerability exploits
D. A worldwide collaborative security network

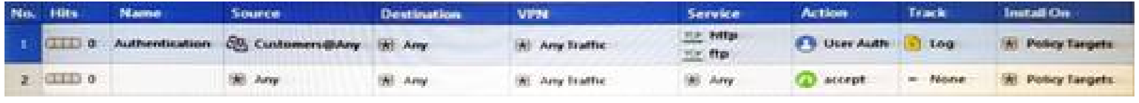
Answer: D

NEW QUESTION 246
- (Exam Topic 3)
Which of the following actions do NOT take place in IKE Phase 1?

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

Answer: B

NEW QUESTION 249
- (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 250
- (Exam Topic 3)
Which remote Access Solution is clientless?

A. Checkpoint Mobile
B. Endpoint Security Suite
C. SecuRemote
D. Mobile Access Portal

Answer: D

NEW QUESTION 255
- (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 259
- (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 262
- (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 266
- (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 271
- (Exam Topic 3)
What happens if the identity of a user is known?

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

Answer: C

NEW QUESTION 276
- (Exam Topic 3)
A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

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

Answer: B

NEW QUESTION 277
- (Exam Topic 3)
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

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

Answer: D

NEW QUESTION 278
- (Exam Topic 3)
As a Security Administrator, you must refresh the Client Authentication authorized time-out every time a new user connection is authorized. How do you do this? Enable the Refreshable Timeout setting:

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

Answer: C

NEW QUESTION 281
- (Exam Topic 3)
You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

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

Answer: C

NEW QUESTION 286
- (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 287
- (Exam Topic 3)
You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

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

Answer: B

NEW QUESTION 288
- (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

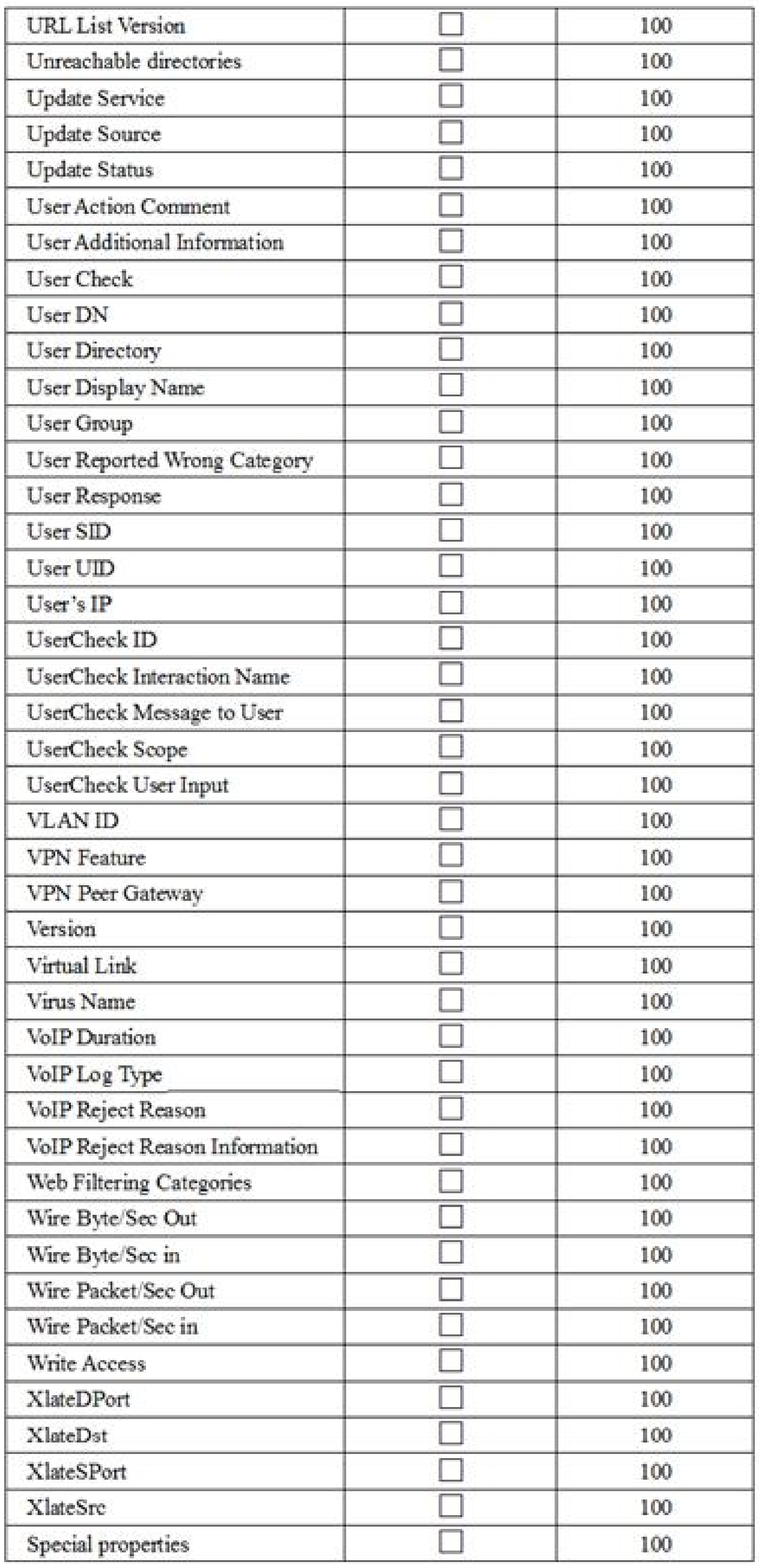
Answer: C

NEW QUESTION 291
- (Exam Topic 3)
You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities sh you do first?

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

Answer: B

NEW QUESTION 296
- (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 299
- (Exam Topic 3)
While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?
1) Select Active Mode tab in SmartView Tracker.
2) Select Tools > Block Intruder.
3) Select Log Viewing tab in SmartView Tracker.
4) Set Blocking Timeout value to 60 minutes.
5) Highlight connection that should be blocked.

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

Answer: C

NEW QUESTION 302
- (Exam Topic 3)
VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

A. 3DES and MD5

B. Certificates and IPsec
C. Certificates and pre-shared secret
D. IPsec and VPN Domains

Answer: C

NEW QUESTION 305
- (Exam Topic 3)
Which set of objects have an Authentication tab?

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

Answer: A

NEW QUESTION 309
- (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 311
- (Exam Topic 3)
Which of the following is NOT an attribute of packer acceleration?

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

Answer: D

NEW QUESTION 315
- (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 320
- (Exam Topic 3)
You are about to integrate RSA SecurID users into the Check Point infrastructure. What kind of users are to be defined via SmartDashboard?

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

Answer: A

NEW QUESTION 325
- (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 326
- (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 329
- (Exam Topic 3)
What is the appropriate default Gaia Portal address?

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

Answer: D

NEW QUESTION 332
- (Exam Topic 3)
When launching SmartDashboard, what information is required to log into R77?

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

Answer: B

NEW QUESTION 336
- (Exam Topic 3)
When defining QoS global properties, which option below is not valid?

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

Answer: C

NEW QUESTION 338
- (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 339
- (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 342
- (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 347

- (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 350
- (Exam Topic 4)
Which of the following commands is used to verify license installation?

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

Answer: B

NEW QUESTION 352
- (Exam Topic 4)
What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?

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

Answer: B

NEW QUESTION 356
- (Exam Topic 4)
Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made:

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

Answer: A

NEW QUESTION 357
- (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 359
- (Exam Topic 4)
The CDT utility supports which of the following?

A. Major version upgrades to R77.30
B. Only Jumbo HFA’s and hotfixes
C. Only major version upgrades to R80.10
D. All upgrades

Answer: D

NEW QUESTION 364
- (Exam Topic 4)
To enforce the Security Policy correctly, a Security Gateway requires:

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

Answer: B

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

NEW QUESTION 365
- (Exam Topic 4)
What is the BEST method to deploy identity Awareness for roaming users?

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

Answer: A

NEW QUESTION 367
- (Exam Topic 4)
Which one of the following is TRUE?

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

Answer: C

NEW QUESTION 372
- (Exam Topic 4)
You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 375
- (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 379
- (Exam Topic 4)
Which identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

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

Answer: D

NEW QUESTION 382
- (Exam Topic 4)
Which of the following is NOT a component of Check Point Capsule?

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

Answer: C

NEW QUESTION 385

- (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 389
- (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

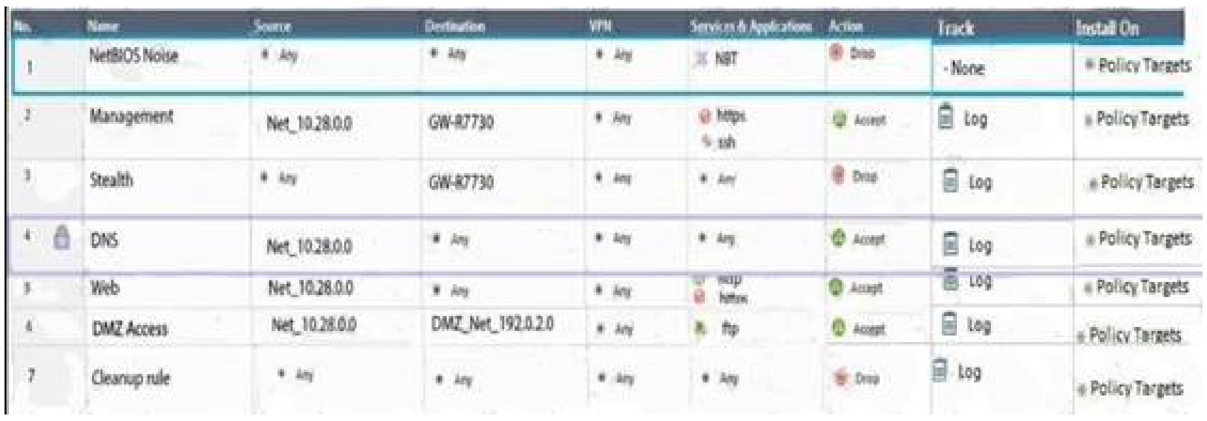
Answer: A

NEW QUESTION 392
- (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 397
- (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.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	Any	Any	Any	NBT	Drop	- None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept	Log	Policy Targets
3	Stealth	Any	GW-R7730	Any	Any	Drop	Log	Policy Targets
4 🔒	DNS	Net_10.28.0.0	Any	Any	Any	Accept	Log	Policy Targets
5	Web	Net_10.28.0.0	Any	Any	http https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	Any	ftp	Accept	Log	Policy Targets
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

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 402
- (Exam Topic 4)
Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays ____ for the given VPN tunnel.

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

Answer: A

NEW QUESTION 406
- (Exam Topic 4)
Which message indicates IKE Phase 2 has completed successfully?

A. Quick Mode Complete
B. Aggressive Mode Complete
C. Main Mode Complete
D. IKE Mode Complete

Answer: A

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

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

Answer: B

NEW QUESTION 415
- (Exam Topic 4)
In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

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

Answer: C

NEW QUESTION 420
- (Exam Topic 4)
What Identity Agent allows packet tagging and computer authentication?

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

Answer: B

NEW QUESTION 423
- (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 428
- (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 430
- (Exam Topic 4)
What is the Transport layer of the TCP/IP model responsible for?

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

Answer: B

NEW QUESTION 431
- (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 435
- (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 437
- (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 442
- (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 445
- (Exam Topic 4)
SmartEvent does NOT use which of the following procedures to identity events:

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

Answer: C

NEW QUESTION 450
- (Exam Topic 4)
Fill the blank. IT is Best Practice to have a _____ rule at the end of each policy layer.

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

Answer: A

NEW QUESTION 454
- (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 458
- (Exam Topic 4)
Which method below is NOT one of the ways to communicate using the Management API's?

A. Typing API commands using the "mgmt_cli" command
B. Typing API commands from a dialog box inside the SmartConsole GUI application

C. Typing API commands using Gaia's secure shell (clash)19+
D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 463
- (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 464
- (Exam Topic 4)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 469
- (Exam Topic 4)
Fill in the blanks. There are _____ types of software containers ______

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

Answer: A

NEW QUESTION 473
- (Exam Topic 4)
When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

A. Distributed
B. Standalone
C. Bridge

Answer: A

NEW QUESTION 478
- (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 481
- (Exam Topic 4)
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

A. Accounting
B. Suppression
C. Accounting/Suppression
D. Accounting/Extended

Answer: C

NEW QUESTION 486
- (Exam Topic 4)
You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

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

Answer: A

NEW QUESTION 487
- (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 488
- (Exam Topic 4)
What is the SOLR database for?

A. Used for full text search and enables powerful matching capabilities
B. Writes data to the database and full text search
C. Serves GUI responsible to transfer request to the DLE server
D. Enables powerful matching capabilities and writes data to the database

Answer: A

NEW QUESTION 493
- (Exam Topic 4)
When an encrypted packet is decrypted, where does this happen?

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

Answer: A

NEW QUESTION 497
- (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 500
- (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 504
- (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 509
- (Exam Topic 4)

Which of the following is NOT a tracking option?

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

Answer: A

NEW QUESTION 512
- (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 513
- (Exam Topic 4)
Fill in the blanks. In ______ NAT, the _______ is translated.

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

Answer: B

NEW QUESTION 515
- (Exam Topic 4)
Fill in the blank: Service blades must be attached to a _____ .

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

Answer: A

NEW QUESTION 520
- (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 521
- (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 524
- (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 526
- (Exam Topic 4)
Which SmartConsole tab is used to monitor network and security performance?

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

Answer: C

NEW QUESTION 528
- (Exam Topic 4)
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

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

Answer: A

NEW QUESTION 530
- (Exam Topic 4)
Phase 1 of the two-phase negotiation process conducted by IKE operates in a_____ mode.

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

Answer: A

NEW QUESTION 535
- (Exam Topic 4)
Which of the following is NOT a valid deployment option for R80?

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

Answer: D

NEW QUESTION 539
- (Exam Topic 4)
What command would show the API server status?

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

Answer: D

NEW QUESTION 541
- (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 543
- (Exam Topic 4)
Which of the following commands is used to monitor cluster members?

A. cphaprob state
B. cphaprob status
C. cphaprob

D. cluster state

Answer: A

NEW QUESTION 545
- (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 548
- (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 552
- (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 556
......