Check-Point

Exam Questions 156-215.80

Check Point Certified Security Administrator

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

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

Answer: D

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

NEW QUESTION 2
- (Exam Topic 1)
What does the “unknown” SIC status shown on SmartConsole mean?

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

Answer: D

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

NEW QUESTION 3
- (Exam Topic 1)
You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

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

Answer: D

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

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

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

Answer: A

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

NEW QUESTION 5
- (Exam Topic 1)
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 6
- (Exam Topic 1)
By default, which port does the WebUI listen on?

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

Answer: C

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

NEW QUESTION 7
- (Exam Topic 1)
When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

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

Answer: D

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

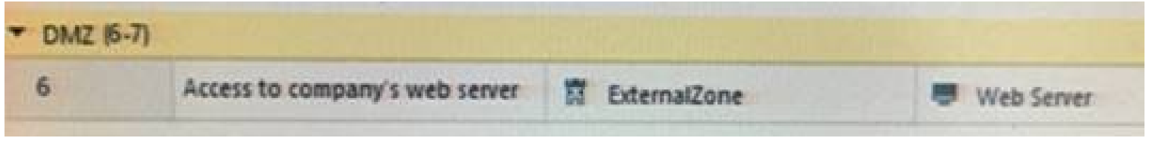
NEW QUESTION 8
- (Exam Topic 1)
While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

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 9
- (Exam Topic 1)
What does ExternalZone represent in the presented rule?

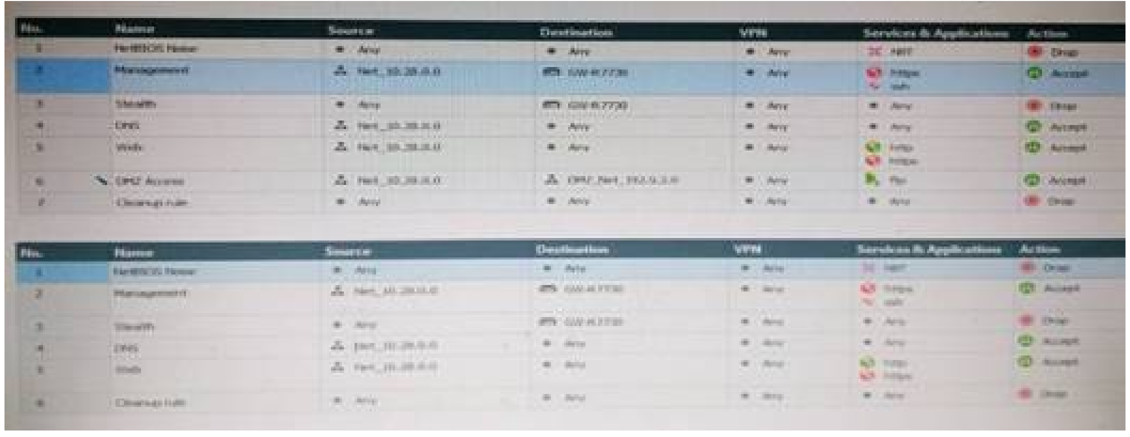

DMZ (6-7)
6 Access to company's web server ExternalZone Web Server

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

Answer: B

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

NEW QUESTION 10
- (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_192.0.2.0	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 10
- (Exam Topic 1)
Which of the following Automatically Generated Rules NAT rules have the lowest implementation priority?

A. Machine Hide NAT
B. Address Range Hide NAT
C. Network Hide NAT
D. Machine Static NAT

Answer: BC

Explanation:
SmartDashboard organizes the automatic NAT rules in this order:
 Static NAT rules for Firewall, or node (computer or server) objects
 Hide NAT rules for Firewall, or node objects
 Static NAT rules for network or address range objects
 Hide NAT rules for network or address range objects
References:

NEW QUESTION 14
- (Exam Topic 1)
What is the default shell for the command line interface?

A. Expert

B. Clish
C. Admin
D. Normal

Answer: B

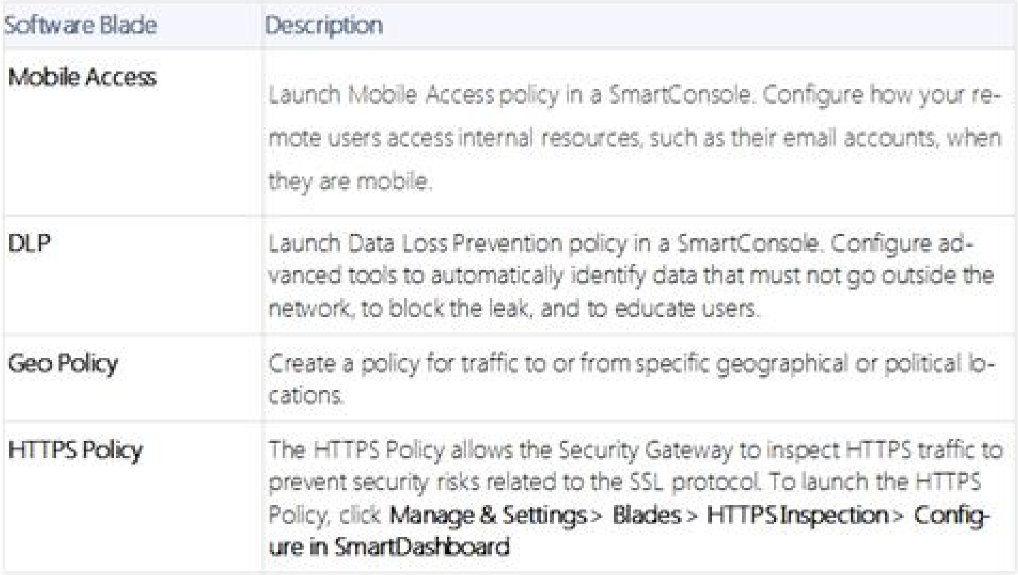
Explanation:
The default shell of the CLI is called clish References:

NEW QUESTION 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

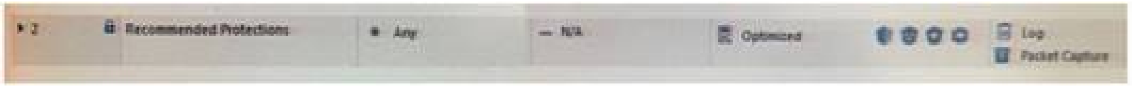
Answer: B

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



2 Recommended Protections Any N/A Optimized Log
Packet Capture

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

Answer: B

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

NEW QUESTION 24
- (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 25

- (Exam Topic 1)

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

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

Answer: D

Explanation:

On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:

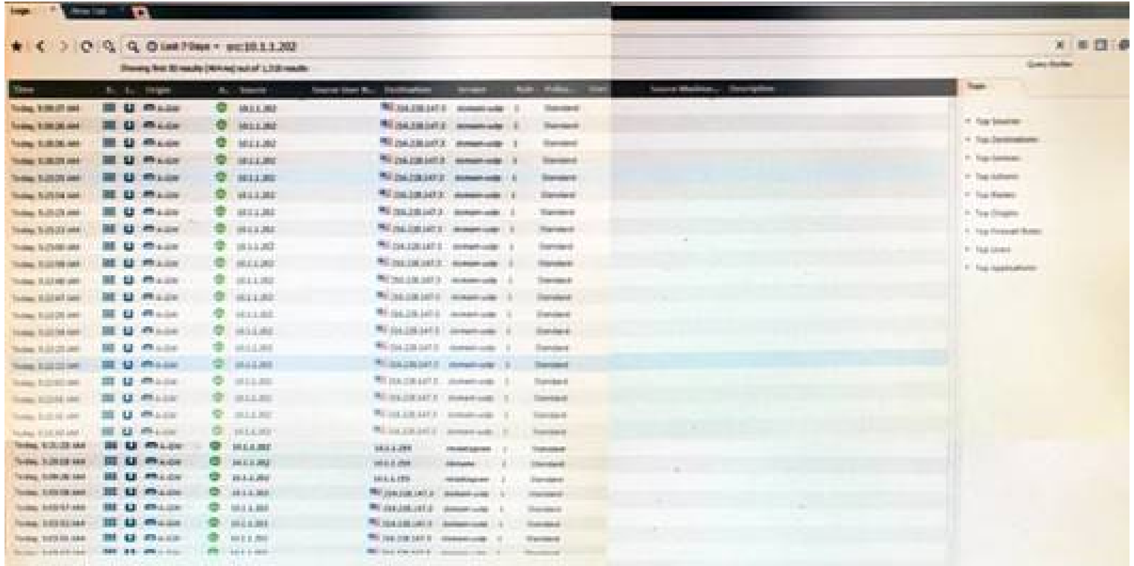
To center and to other Satellites through center; this allows connectivity between Gateways; for example, if the spoke Gateways are DAIP Gateways, and the hub is a Gateway with a static IP address

To center, or through the center to other satellites, to Internet and other VPN targets; this allows connectivity between the Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

NEW QUESTION 28

- (Exam Topic 1)

The following graphic shows:



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

Answer: C

NEW QUESTION 29

- (Exam Topic 1)

Which of the following is NOT a license activation method?

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

Answer: A

NEW QUESTION 31

- (Exam Topic 1)

In R80, Unified Policy is a combination of

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

Answer: D

Explanation:

D is the best answer given the choices. Unified Policy

In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

Firewall and VPN
Application Control and URL Filtering
Identity Awareness
Data Awareness
Mobile Access

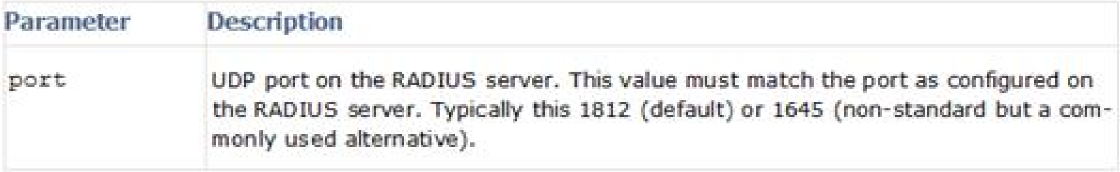
Security Zones

NEW QUESTION 33
- (Exam Topic 1)
Fill in the blank: RADIUS protocol uses ______ to communicate with the gateway.

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

Answer: A

Explanation:
Parameters:



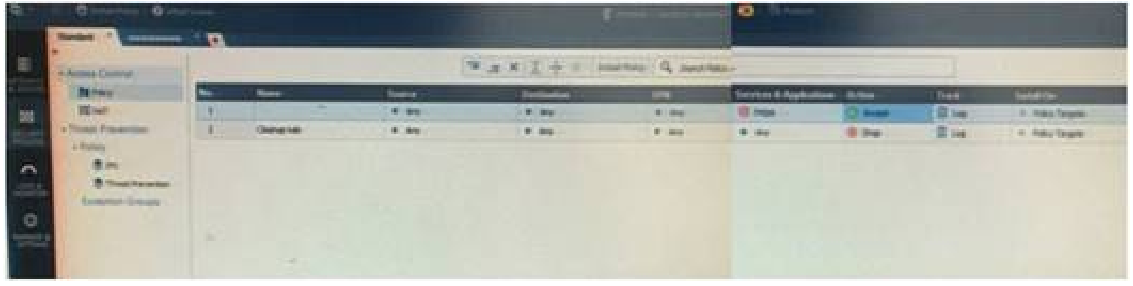
Parameter	Description
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).

NEW QUESTION 35
- (Exam Topic 1)
In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

A. Display policies and logs on the administrator's workstation.
B. Verify and compile Security Policies.
C. Processing and sending alerts such as SNMP traps and email notifications.
D. Store firewall logs to hard drive storage.

Answer: A

NEW QUESTION 39
- (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 40
- (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 41
- (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 42
- (Exam Topic 1)
The security Gateway is installed on GAiA R80 The default port for the WEB User Interface is ____.

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

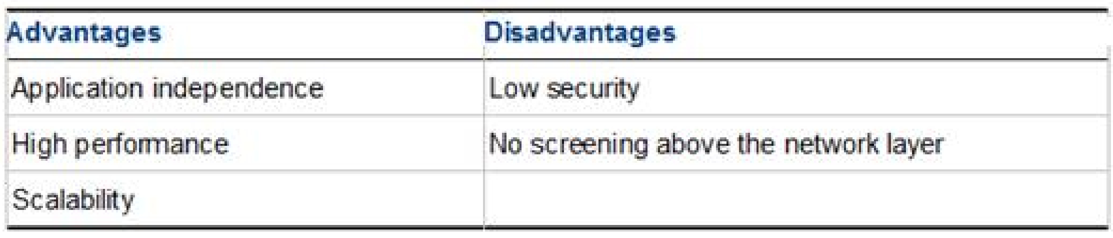
Answer: D

NEW QUESTION 47
- (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	

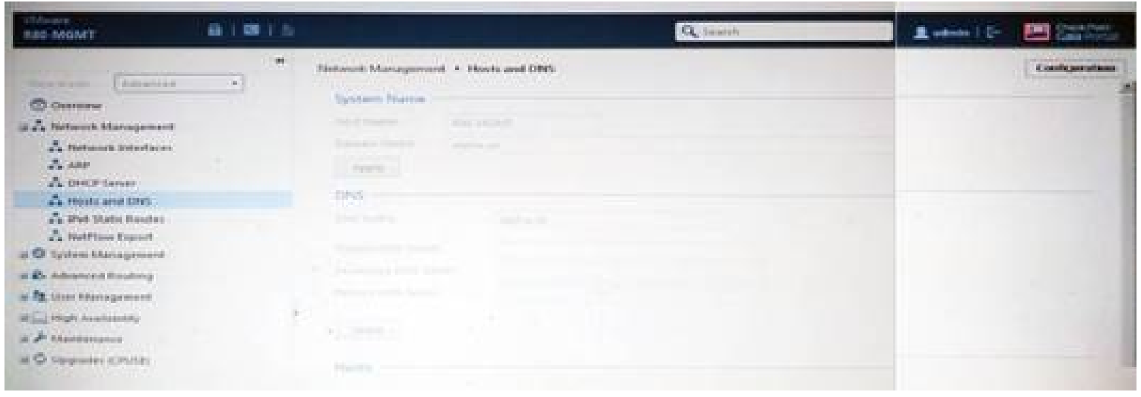
NEW QUESTION 52
- (Exam Topic 1)
To optimize Rule Base efficiency, the most hit rules should be where?

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 53
- (Exam Topic 1)
ABC Corp has a new administrator who logs into the Gaia Portal to make some changes. He realizes that even though he has logged in as an administrator, he is unable to make any changes because all configuration options are greyed out as shown in the screenshot image below. What is the likely cause for this?



A. The Gaia /bin/confd is locked by another administrator from a SmartConsole session.
B. The database is locked by another administrator SSH session.
C. The Network address of his computer is in the blocked hosts.
D. The IP address of his computer is not in the allowed hosts.

Answer: B

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

NEW QUESTION 58
- (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.

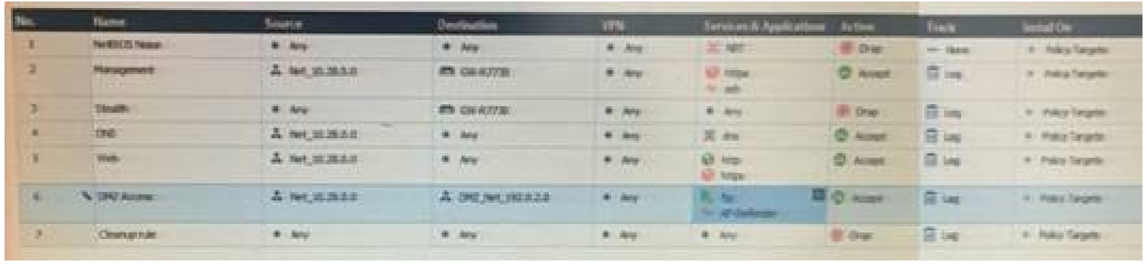
NEW QUESTION 59
- (Exam Topic 1)
Which Threat Prevention Software Blade provides comprehensive against malicious and unwanted network traffic, focusing on application and server vulnerabilities?

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 62
- (Exam Topic 1)
You are the administrator for ABC Corp. You have logged into your R80 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.



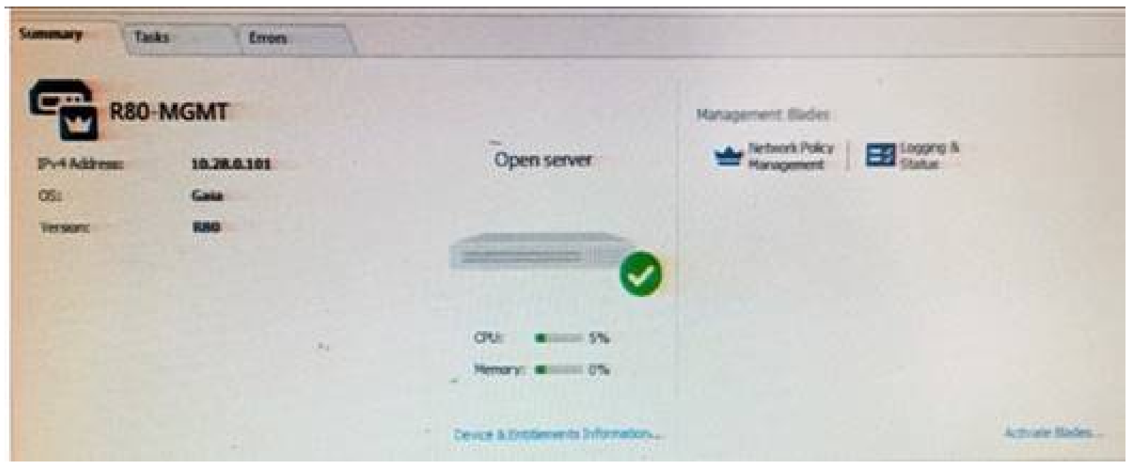
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	Any	Any	Any	NBT	Drop	None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept	Log	Policy Targets
3	Stealth	Any	GW-R7730	Any	Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	Any	Any	dns	Accept	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 AP-Defender	Accept	Log	Policy Targets
7	Cleanup rule	Any	Any	Any	Any	Drop	Log	Policy Targets

What does this mean?

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

Answer: C

NEW QUESTION 63
- (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

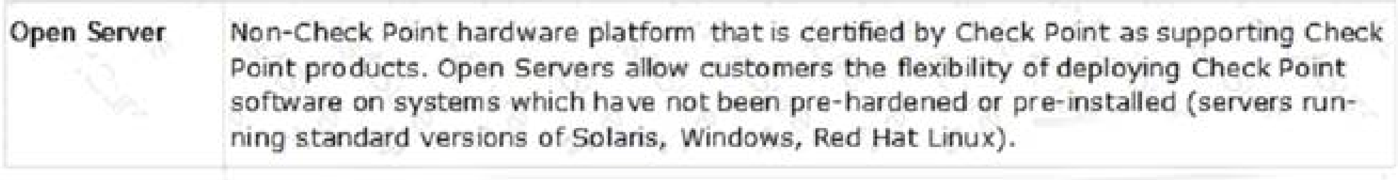
CPU: 5%
Memory: 0%

Management Blades
Network Policy Management
Logging & Status

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 67
- (Exam Topic 2)
What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

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

Answer: A

NEW QUESTION 71
- (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 74
- (Exam Topic 2)
To install a brand new Check Point Cluster, the MegaCorp IT department bought 1 Smart-1 and 2 Security Gateway Appliances to run a cluster. Which type of cluster is it?

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

Answer: B

NEW QUESTION 76
- (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 78
- (Exam Topic 2)
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is ___ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

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

Answer: D

NEW QUESTION 82
- (Exam Topic 2)
Fill in the blanks: The Application Layer Firewalls inspect traffic through the ____ layer(s) of the TCP/IP model and up to and including the ____ layer.

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

Answer: A

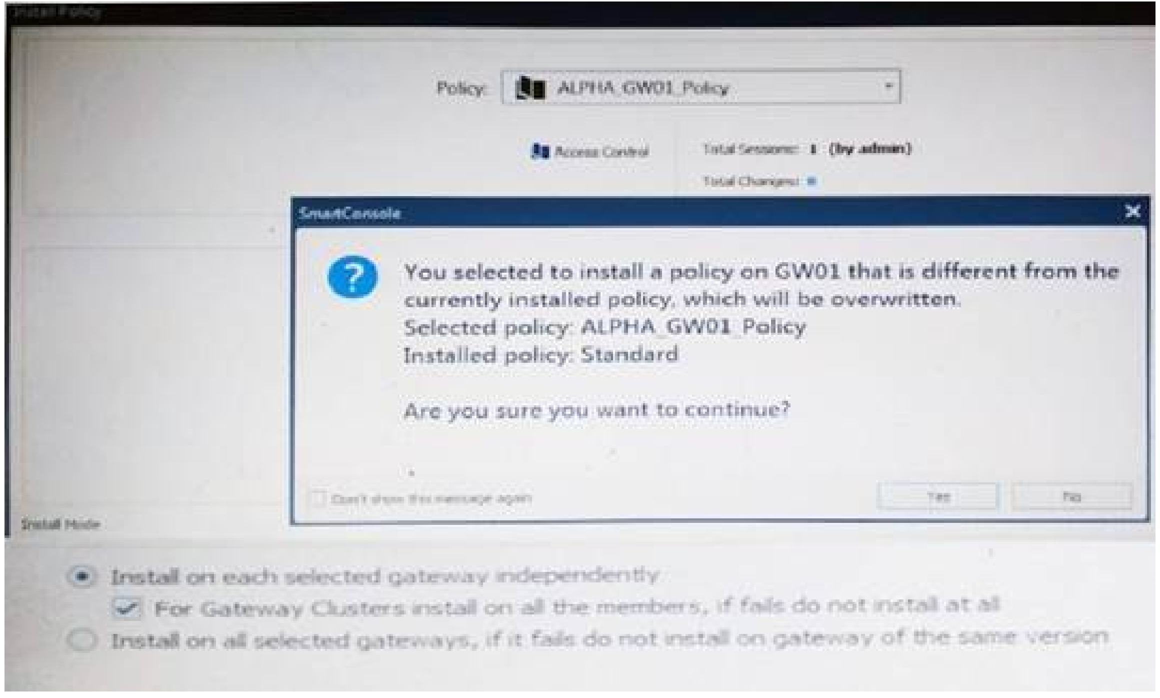
NEW QUESTION 84
- (Exam Topic 2)
Which of the following is NOT an alert option?

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 89
- (Exam Topic 2)
Why would an administrator see the message below?



Policy: ALPHA_GW01_Policy

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?

● 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 91
- (Exam Topic 2)
Which of the following is NOT a back up method?

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

Answer: A

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

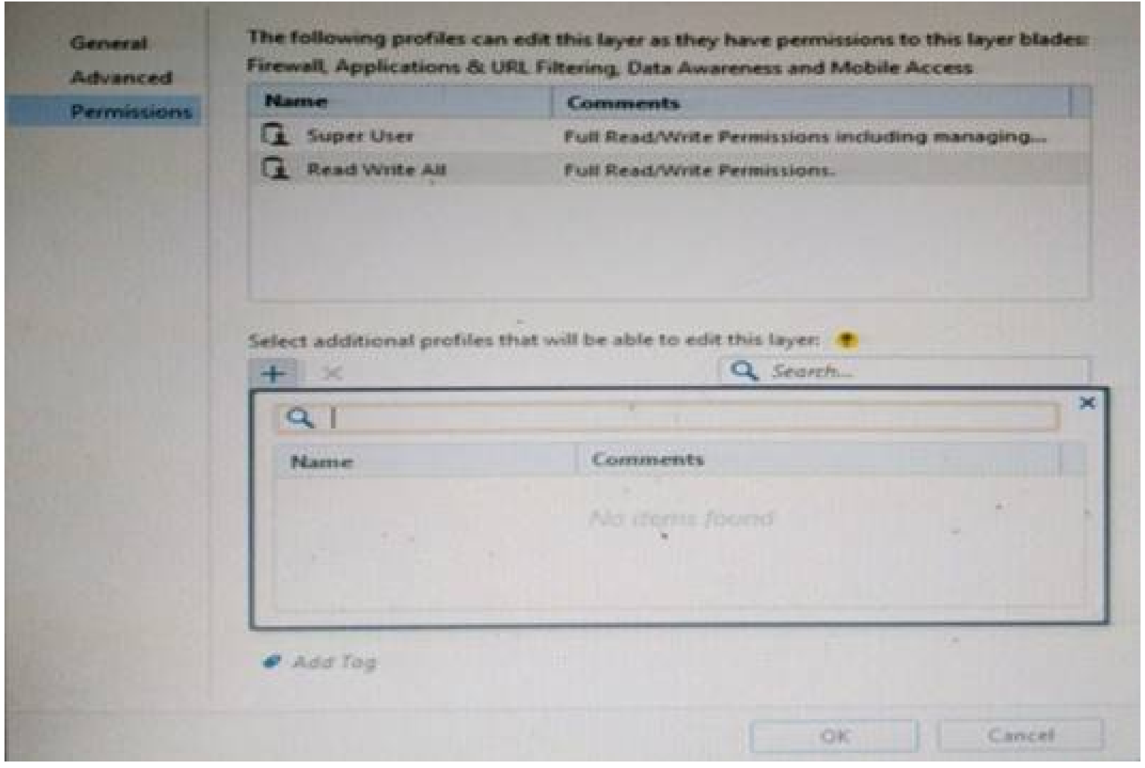
NEW QUESTION 94
- (Exam Topic 2)
Which of the following is NOT a VPN routing option available in a star community?

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 98
- (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:

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 102
- (Exam Topic 2)
Fill in the blank: A ____ is used by a VPN gateway to send traffic as if it were a physical interface.

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

Answer: A

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

NEW QUESTION 107
- (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 109
- (Exam Topic 2)
Fill in the blank: A(n) _____ rule is created by an administrator and is located before the first and before last rules in the Rule Base.

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

Answer: E

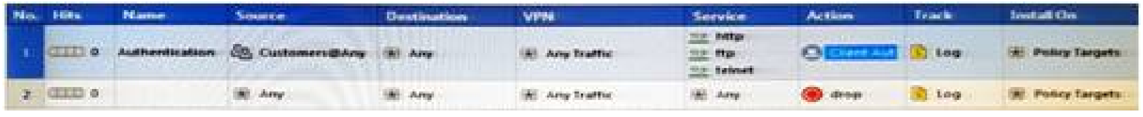
Explanation:
This is the order that rules are enforced:
First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.
Explicit Rules: These are rules that you create.
Before Last Implied Rules: These implied rules are applied before the last explicit rule.
Last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

NEW QUESTION 111
- (Exam Topic 2)
Which directory holds the SmartLog index files by default?

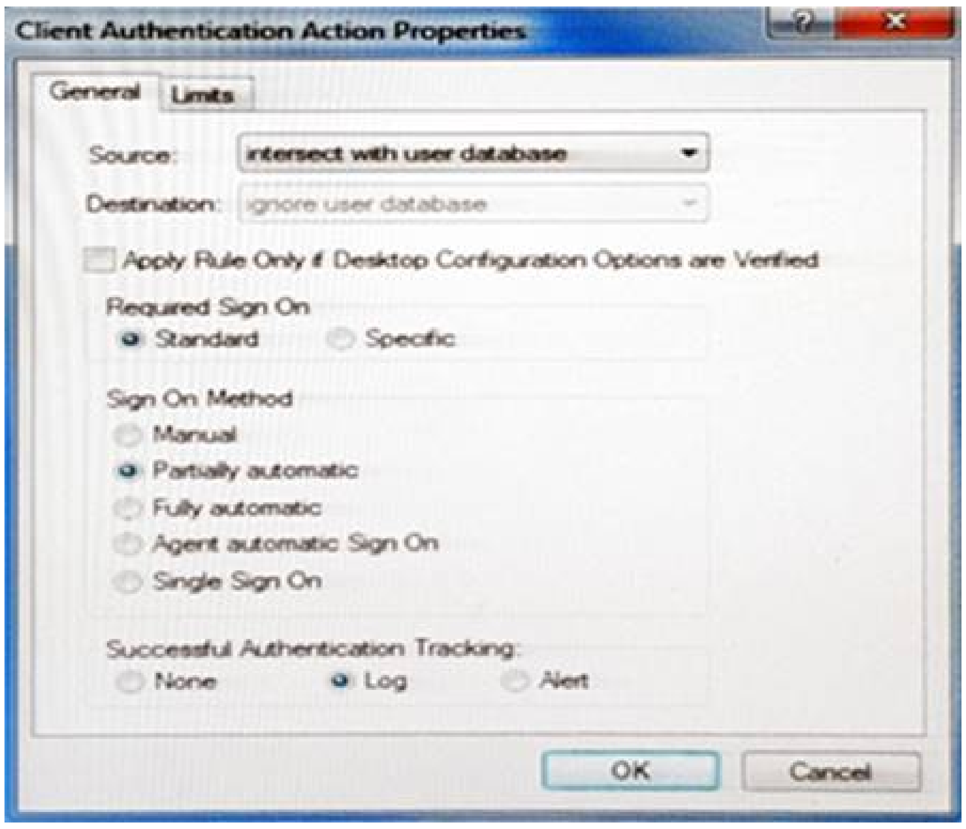
A. $SMARTLOGDIR/data
B. $SMARTLOG/dir
C. $FWDIR/smartlog
D. $FWDIR/log

Answer: A

NEW QUESTION 114
- (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



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 117
- (Exam Topic 2)
Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

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

Answer: D

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

NEW QUESTION 119
- (Exam Topic 2)
Joey is using the computer with IP address 192.168.20.13. He wants to access web page “www.Check Point.com”, which is hosted on Web server with IP address 203.0.113.111. How many rules on Check Point Firewall are required for this connection?

A. Two rules – first one for the HTTP traffic and second one for DNS traffic.
B. Only one rule, because Check Point firewall is a Packet Filtering firewall
C. Two rules – one for outgoing request and second one for incoming replay.
D. Only one rule, because Check Point firewall is using Stateful Inspection technology.

Answer: D

NEW QUESTION 124
- (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 129
- (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 133
- (Exam Topic 2)
What is the default method for destination NAT?

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

Answer: D

NEW QUESTION 138
- (Exam Topic 2)
What happens if the identity of a user is known?

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

Answer: D

NEW QUESTION 141
- (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 145
- (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 147
- (Exam Topic 2)
The IT Management team is interested in the new features of the Check Point R80 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80 because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

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

Answer: A

NEW QUESTION 151
- (Exam Topic 2)
Which information is included in the “Full Log” tracking option, but is not included in the “Log” tracking option?

A. file attributes

B. application information
C. destination port
D. data type information

Answer: D

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

NEW QUESTION 152
- (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 157
- (Exam Topic 2)
AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule? Choose the BEST answer.

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

Answer: C

NEW QUESTION 161
- (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 165
- (Exam Topic 2)
How many users can have read/write access in Gaia at one time?

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

Answer: B

NEW QUESTION 169
- (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

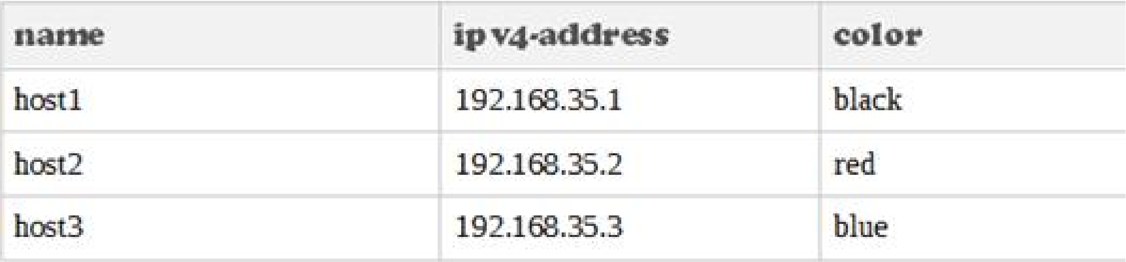
Explanation:
Endpoint Identity Agents – dedicated client agents installed on users' computers that acquire and report identities to the Security Gateway.

NEW QUESTION 173
- (Exam Topic 2)
Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?

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

Answer: A

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



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

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

NEW QUESTION 178
- (Exam Topic 2)
The organization's security manager wishes to back up just the Gaia operating system parameters. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries?

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

Answer: B

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

NEW QUESTION 180
- (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 185
- (Exam Topic 3)
Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

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

Answer: B

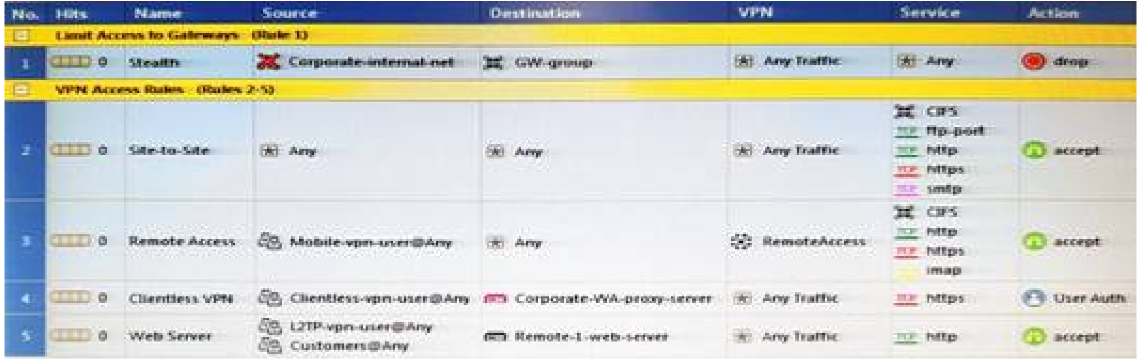
NEW QUESTION 189
- (Exam Topic 3)
What is the mechanism behind Threat Extraction?

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 192
- (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 195
- (Exam Topic 3)
Which is the correct order of a log flow processed by SmartEvent components:

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

Answer: D

NEW QUESTION 200
- (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 204
- (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 208
- (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 210
- (Exam Topic 3)

To fully enable Dynamic Dispatcher on a Security Gateway:

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

Answer: A

NEW QUESTION 215
- (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 216
- (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 217
- (Exam Topic 3)
Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

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

Answer: B

NEW QUESTION 220
- (Exam Topic 3)
Which of the following is NOT an option for internal network definition of Anti-spoofing?

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

Answer: B

NEW QUESTION 225
- (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 226
- (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 229
- (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 234
- (Exam Topic 3)
On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

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

Answer: B

NEW QUESTION 235
- (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 236
- (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 240
- (Exam Topic 3)
Which of the following firewall modes DOES NOT allow for Identity Awareness to be deployed?

A. Bridge
B. Load Sharing
C. High Availability
D. Fail Open

Answer: A

NEW QUESTION 241
- (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 243
- (Exam Topic 3)
What is the command to see cluster status in cli expert mode?

A. fw ctl stat
B. clusterXL stat
C. clusterXL status
D. cphaprob stat

Answer:

A

NEW QUESTION 247
- (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 252
- (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 253
- (Exam Topic 3)
According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added? A(n):

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

Answer: C

NEW QUESTION 255
- (Exam Topic 3)
Which NAT rules are prioritized first?

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

Answer: B

NEW QUESTION 258
- (Exam Topic 3)
Which of the following is a hash algorithm?

A. 3DES
B. IDEA
C. DES
D. MD5

Answer: D

NEW QUESTION 261
- (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 262
- (Exam Topic 3)
Which R77 GUI would you use to see number of packets accepted since the last policy install?

A. SmartView Monitor
B. SmartView Tracker
C. SmartDashboard

D. SmartView Status

Answer: A

NEW QUESTION 267
- (Exam Topic 3)
All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

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

Answer: B

NEW QUESTION 270
- (Exam Topic 3)
Identify the API that is not supported by Check Point currently.

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

Answer: C

NEW QUESTION 275
- (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 277
- (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 279
- (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 280
- (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 282
- (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 286
- (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 287
- (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 291
- (Exam Topic 4)
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

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

Answer: C

NEW QUESTION 296
- (Exam Topic 4)
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

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

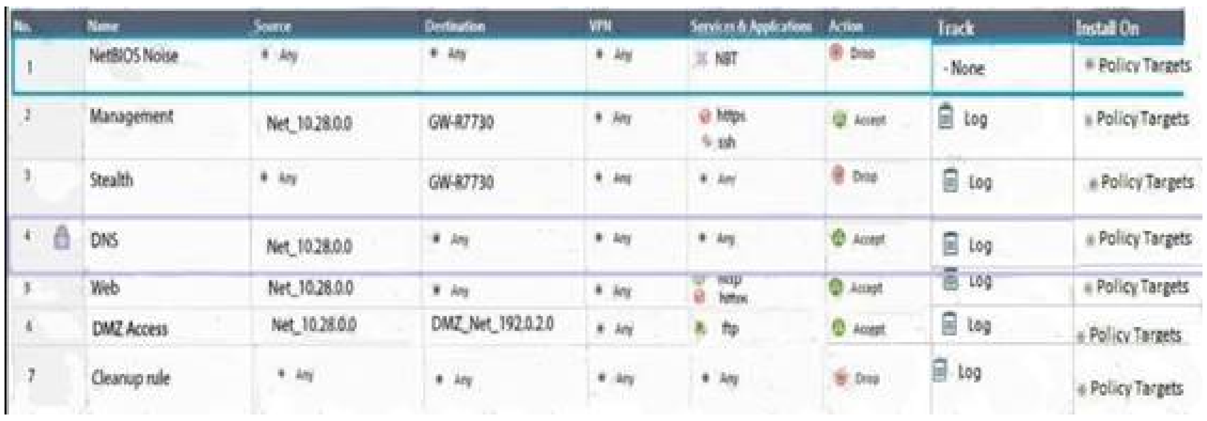
Answer: B

NEW QUESTION 298
- (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 299
- (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 304
- (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 308
- (Exam Topic 4)
The SIC Status “Unknown” means

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

Answer: CExplanation:SICStatus

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

NEW QUESTION 310
- (Exam Topic 4)
Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Answer: B

NEW QUESTION 313
- (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 318
- (Exam Topic 4)
What is the purpose of the Clean-up Rule?

A. To log all traffic that is not explicitly allowed or denied in the Rule Base.

B. To clean up policies found inconsistent with the compliance blade reports.
C. To remove all rules that could have a conflict with other rules in the database.
D. To eliminate duplicate log entries in the Security Gateway

Answer: A

NEW QUESTION 320
- (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 325
- (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 330
- (Exam Topic 4)
Fill in the blank: To create policy for traffic to or from a particular location, use the_____ .

A. DLP shared policy
B. Geo policy shared policy
C. Mobile Access software blade
D. HTTPS inspection

Answer: B

Explanation:
Shared Policies
The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. T are shared between all Policy packages.
Shared policies are installed with the Access Control Policy. Software Blade
Description Mobile Access
Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy
Create a policy for traffic to or from specific geographical or political locations. References:

NEW QUESTION 335
- (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 338
- (Exam Topic 4)
When configuring LDAP User Directory integration, Changes applied to a User Directory template are:

A. Reflected immediately for all users who are using template.
B. Not reflected for any users unless the local user template is changed.
C. Reflected for all users who are using that template and if the local user template is changed as well.
D. Not reflected for any users who are using that template.

Answer: A

Explanation:
The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local.
You can change the User Directory templates. Users
associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.

NEW QUESTION 343
- (Exam Topic 4)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 344
- (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 345
- (Exam Topic 4)
What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

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

Answer: D

NEW QUESTION 348
- (Exam Topic 4)
You have discovered activity in your network. What is the BEST immediate action to take?

A. Create a policy rule to block the traffic.
B. Create a suspicious action rule to block that traffic.
C. Wait until traffic has been identified before making any changes.
D. Contact ISP to block the traffic.

Answer: B

NEW QUESTION 349
- (Exam Topic 4)
Fill in the blank: An LDAP server holds one or more ______.

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

Answer: C

NEW QUESTION 352
- (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 357
- (Exam Topic 4)
Which GUI tool can be used to view and apply Check Point licenses?

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

Answer: D

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

NEW QUESTION 359
- (Exam Topic 4)
Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

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

Answer: A

NEW QUESTION 363
- (Exam Topic 4)
Which statement is NOT TRUE about Delta synchronization?

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

Answer: A

NEW QUESTION 367
- (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 370
- (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 374
- (Exam Topic 4)
Which path below is available only when CoreXL is enabled?

A. Slow path
B. Firewall path
C. Medium path
D. Accelerated path

Answer: C

NEW QUESTION 377
- (Exam Topic 4)
To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
C. cphaprob –a if
D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Answer: B

NEW QUESTION 378
......

Relate Links

100% Pass Your 156-215.80 Exam with Exambible Prep Materials

https://www.exambible.com/156-215.80-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/