Check-Point

Exam Questions 156-215.80

Check Point Certified Security Administrator

NEW QUESTION 1
- (Exam Topic 1)
Which of the following technologies extracts detailed information from packets and stores that information in state tables?

A. INSPECT Engine
B. Stateful Inspection
C. Packet Filtering
D. Application Layer Firewall

Answer: B

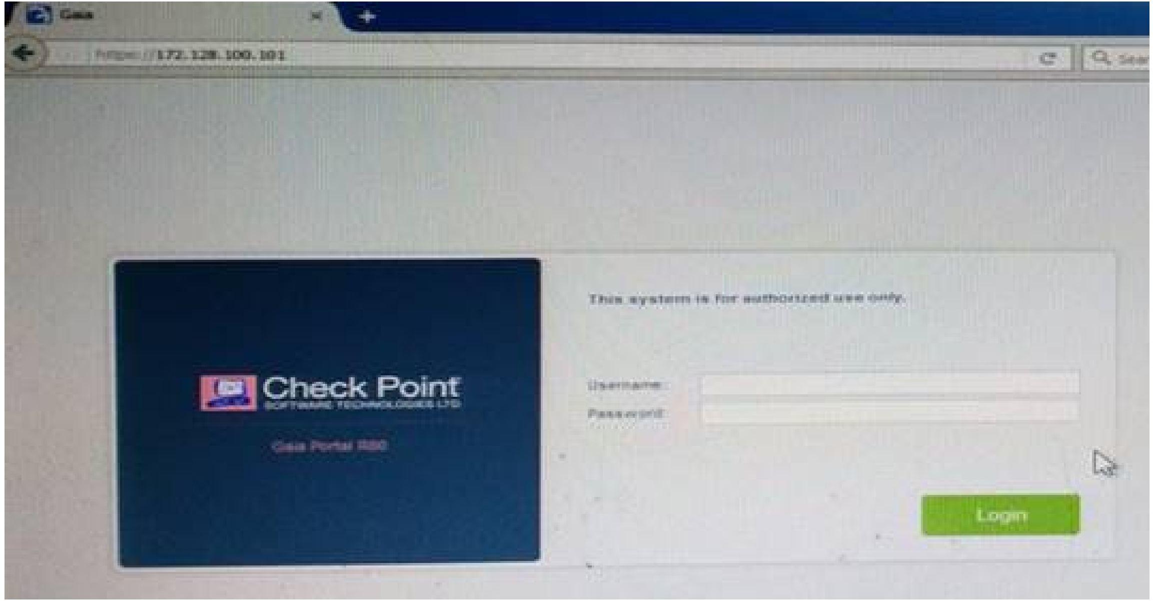
NEW QUESTION 2
- (Exam Topic 1)
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

A. UserCheck
B. Active Directory Query
C. Account Unit Query
D. User Directory Query

Answer: B

Explanation:
AD Query extracts user and computer identity information from the Active Directory Security Event Logs. The system generates a Security Event log entry when a user or computer accesses a network resource. For example, this occurs when a user logs in, unlocks a screen, or accesses a network drive.
Reference : https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

NEW QUESTION 3
- (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:

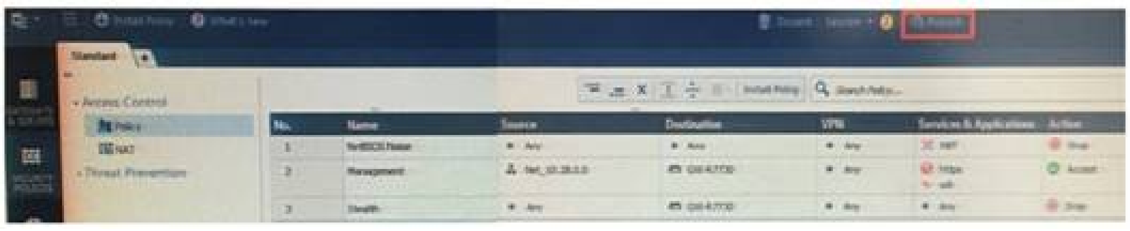
NEW QUESTION 4
- (Exam Topic 1)
Fill in the blank: The R80 utility fw monitor is used to troubleshoot _______

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 5
- (Exam Topic 1)
ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house R80 Management to the other administrators in ABC Corp.



No.	Name	Source	Destination	VPN	Services & Applications	Action
1	NetBIOS Noise	Any	Any	Any	NBT	Drop
2	Management	[illegible]	[illegible]	Any	https ssh	Accept
3	Stealth	Any	[illegible]	Any	Any	Drop

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

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

Answer: C

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

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

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

Answer: A

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

NEW QUESTION 7
- (Exam Topic 1)
Joey wants to configure NTP on R80 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

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

Answer: A

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

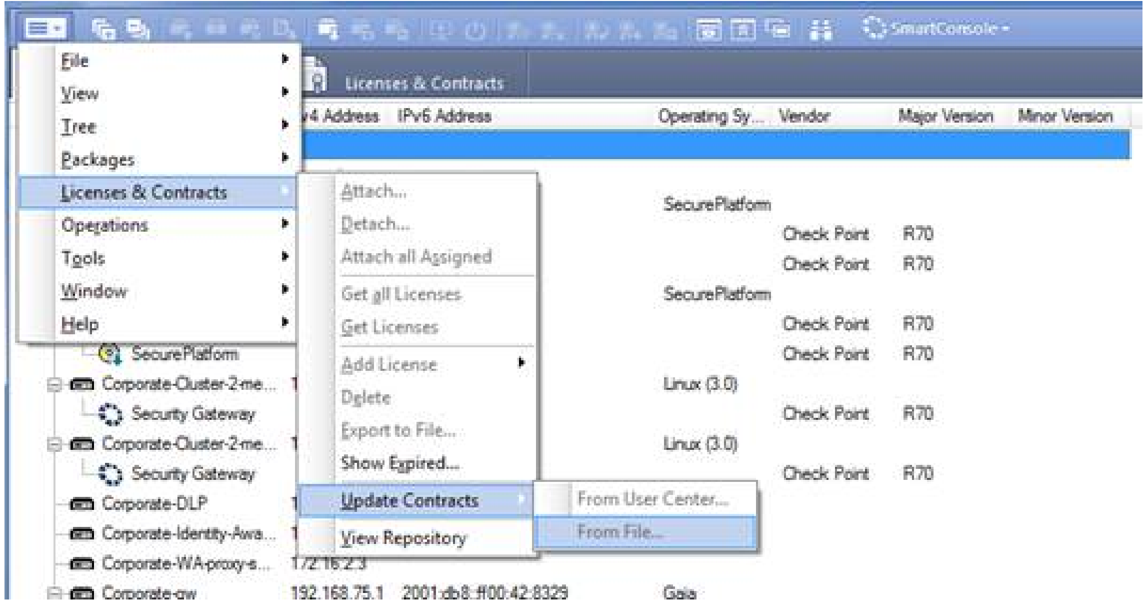
NEW QUESTION 8
- (Exam Topic 1)
Which application should you use to install a contract file?

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 9
- (Exam Topic 1)
Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 1)
What are the three authentication methods for SIC?

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

Answer: B

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

NEW QUESTION 10
- (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 14
- (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 16
- (Exam Topic 1)
When attempting to start a VPN tunnel, in the logs the error 'no proposal chosen' is seen numerous times. No other VPN-related log entries are present. Which phase of the VPN negotiations has failed?

A. IKE Phase 1
B. IPSEC Phase 2
C. IPSEC Phase 1
D. IKE Phase 2

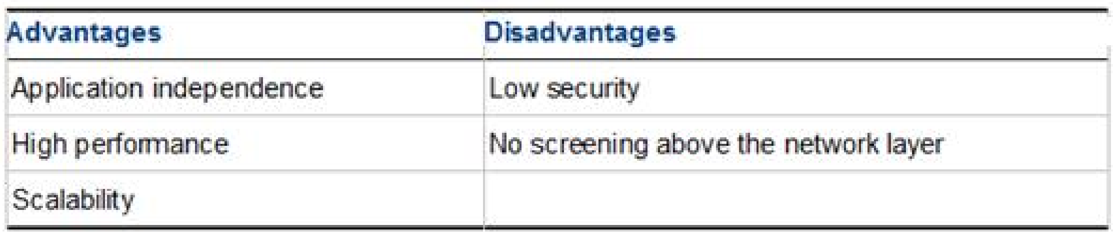
Answer: D

NEW QUESTION 19
- (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 23
- (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.

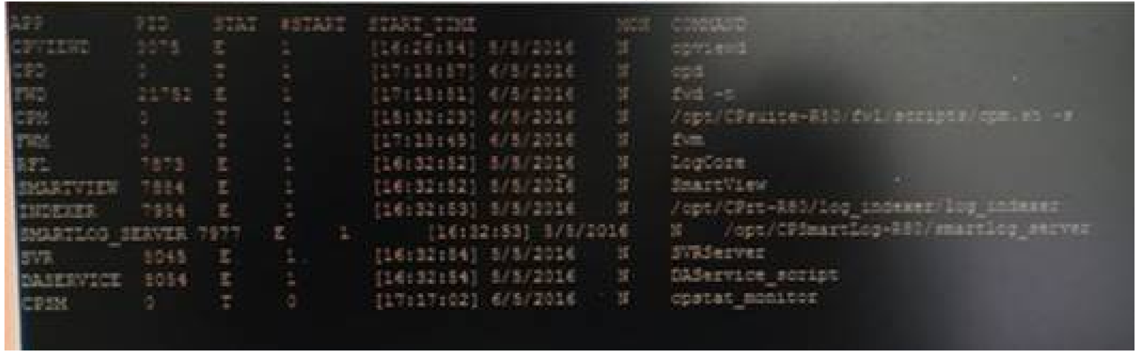
NEW QUESTION 24
- (Exam Topic 1)
What are the two high availability modes?

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

Answer: D

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

NEW QUESTION 26
- (Exam Topic 1)
You are unable to login to SmartDashboard. You log into the management server and run #cpwd_admin list with the following output:



```
APP              PID    STAT  #START  START_TIME            MON  COMMAND
CPVIEWD          5078   E     1       [16:28:54] 5/5/2016   N    cpviewd
CPD              0      T     1       [17:13:57] 4/5/2016   N    cpd
FWD              21752  E     1       [17:13:51] 4/5/2016   N    fwd -n
CPM              0      T     1       [18:32:23] 4/5/2016   N    /opt/CPsuite-R80/fw1/scripts/cpm.sh -s
FWM              0      T     1       [17:13:45] 4/5/2016   N    fwm
RFL              7873   E     1       [16:32:52] 5/5/2016   N    LogCore
SMARTVIEW        7884   E     1       [16:32:52] 5/5/2016   N    SmartView
INDEXER          7954   E     1       [16:32:53] 5/5/2016   N    /opt/CPrt-R80/log_indexer/log_indexer
SMARTLOG_SERVER 7977   E     1       [16:32:53] 5/5/2016   N    /opt/CPSmartLog-R80/smartlog_server
SVR              8045   E     1       [16:32:54] 5/5/2016   N    SVRServer
DASERVICE        8054   E     1       [16:32:54] 5/5/2016   N    DAService_script
CPSM             0      T     0       [17:17:02] 6/5/2016   N    cpstat_monitor
```

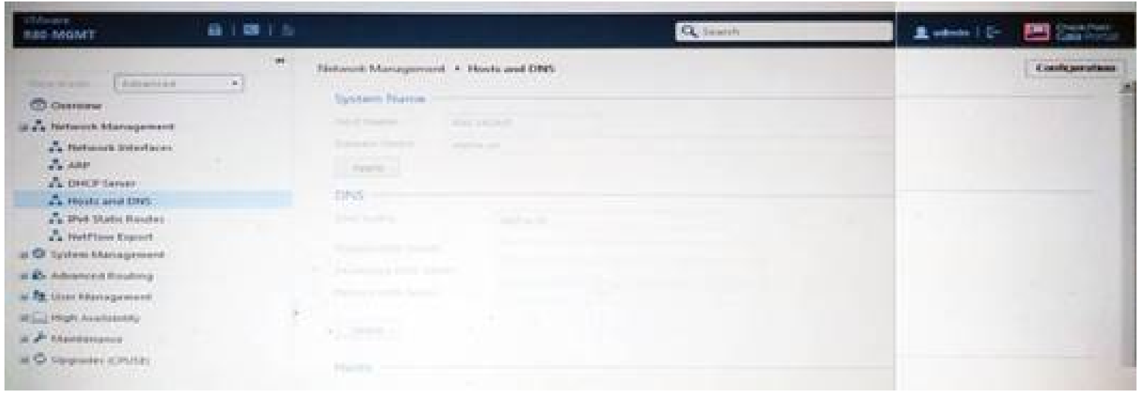
What reason could possibly BEST explain why you are unable to connect to SmartDashboard?

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

Answer: C

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

NEW QUESTION 31
- (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 34
- (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 36
- (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

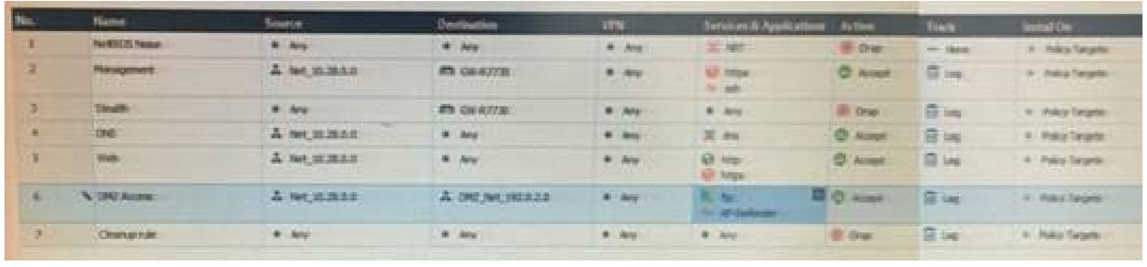
NEW QUESTION 39
- (Exam Topic 1)
Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address?

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 42
- (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

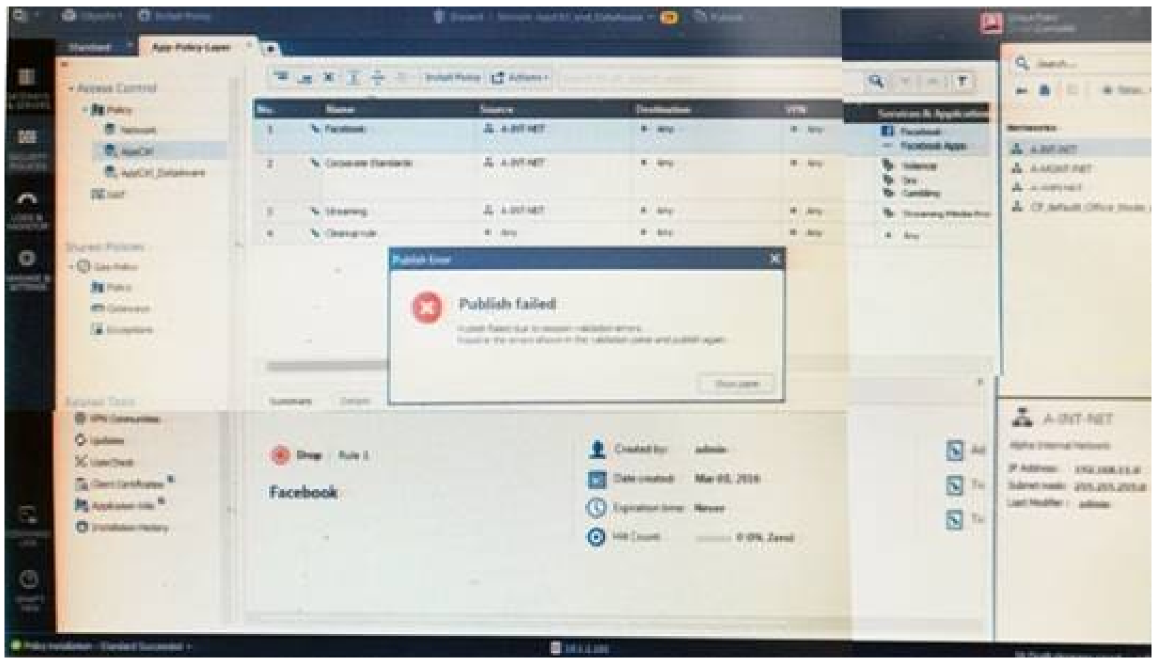
NEW QUESTION 44
- (Exam Topic 1)
What are the two types of address translation rules?

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

Answer: D

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

NEW QUESTION 49
- (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

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

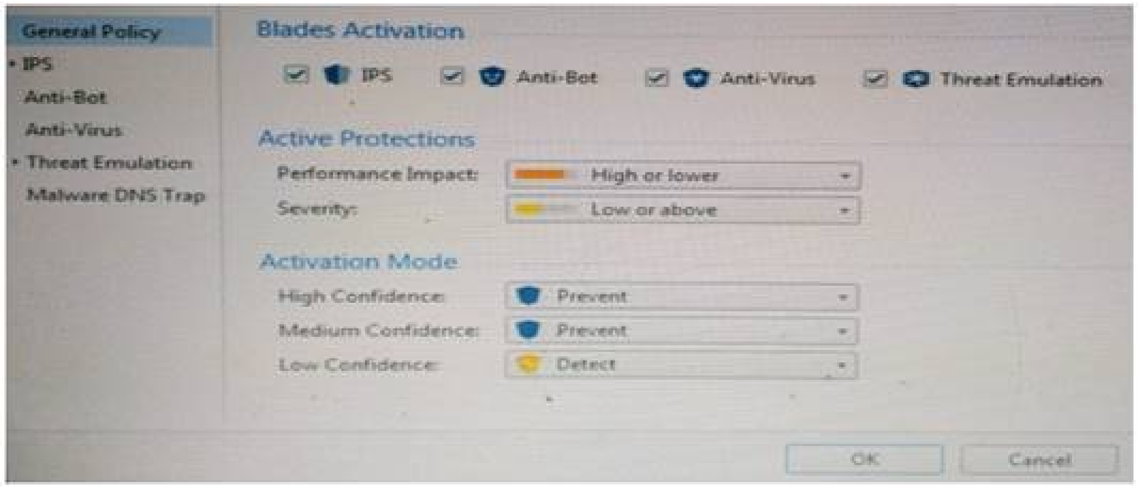
Explanation:
Validation Errors
The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.
To publish, you must fix the errors.

NEW QUESTION 53
- (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 57
- (Exam Topic 2)
Provide very wide coverage for all products and protocols, with noticeable performance impact.



General Policy
- IPS
Anti-Bot
Anti-Virus
- Threat Emulation
Malware DNS Trap

Blades Activation
☑ IPS ☑ Anti-Bot ☑ Anti-Virus ☑ Threat Emulation

Active Protections
Performance Impact: High or lower
Severity: Low or above

Activation Mode
High Confidence: Prevent
Medium Confidence: Prevent
Low Confidence: Detect

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

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

Answer: B

NEW QUESTION 60
- (Exam Topic 2)
Which of the following is NOT an element of VPN Simplified Mode and VPN Communities?

A. “Encrypt” action in the Rule Base
B. Permanent Tunnels
C. “VPN” column in the Rule Base
D. Configuration checkbox “Accept all encrypted traffic”

Answer: A

Explanation:
Migrating from Traditional Mode to Simplified Mode
To migrate from Traditional Mode VPN to Simplified Mode:
1. On the Global Properties > VPN page, select one of these options:
• Simplified mode to all new Firewall Policies
• Traditional or Simplified per new Firewall Policy
2. Click OK.
3. From the R80 SmartConsole Menu, select Manage policies. The Manage Policies window opens.
4. Click New.
The New Policy window opens.
5. Give a name to the new policy and select Access Control.
In the Security Policy Rule Base, a new column marked VPN shows and the Encrypt option is no longer available in the Action column. You are now working in Simplified Mode.

NEW QUESTION 65
- (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 69
- (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 74
- (Exam Topic 2)
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

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

Answer: D

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

NEW QUESTION 79
- (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 84
- (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 87
- (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 88
- (Exam Topic 2)
If there is an Accept Implied Policy set to “First”, what is the reason Jorge cannot see any logs?

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

Answer: A

Explanation:
Implied Rules are configured only on Global Properties.

NEW QUESTION 90
- (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

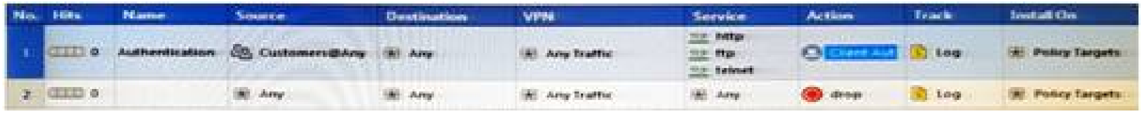
Explanation:
This is the order that rules are enforced:
First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.
Explicit Rules: These are rules that you create.
Before Last Implied Rules: These implied rules are applied before the last explicit rule.
Last 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 92
- (Exam Topic 2)
In order to modify Security Policies the administrator can use which of the following tools? Select the BEST answer.

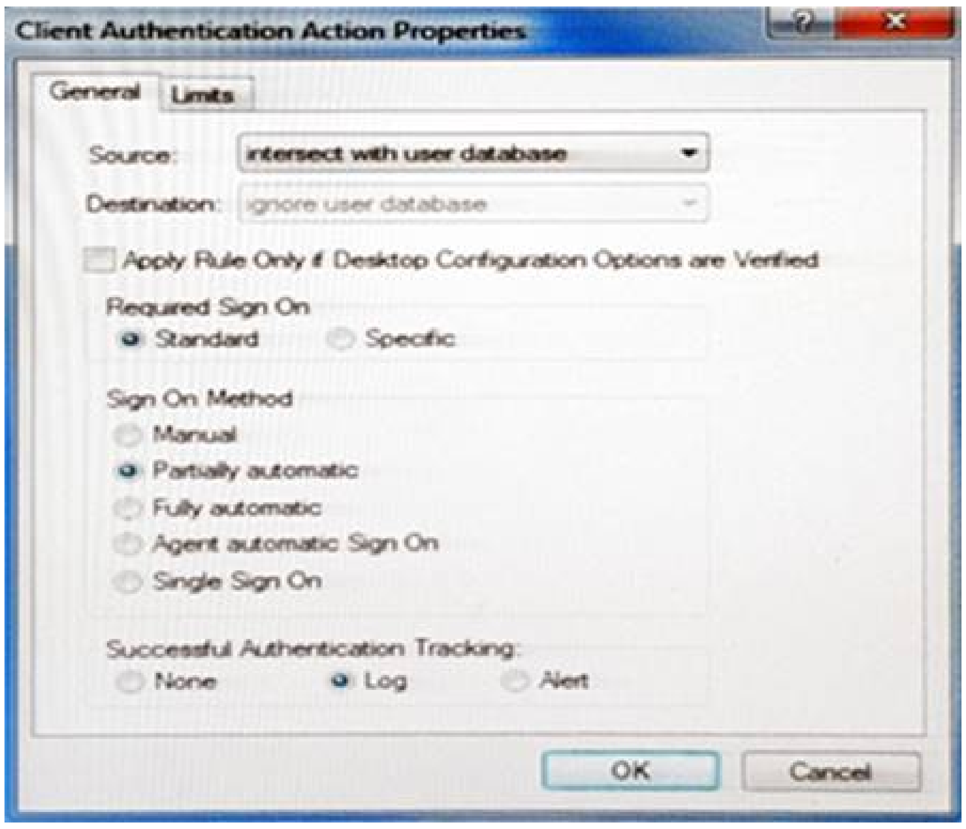
A. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
B. SmartConsole and WebUI on the Security Management Server.
C. mgmt_cli or WebUI on Security Gateway and SmartConsole on the Security Management Server.
D. SmartConsole or mgmt_cli on any computer where SmartConsole is installed.

Answer: D

NEW QUESTION 96
- (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

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 101
- (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 105
- (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 108
- (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 110
- (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 113
- (Exam Topic 2)
Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

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

Answer: D

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

NEW QUESTION 115
- (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 120
- (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 124
- (Exam Topic 2)
NAT can NOT be configured on which of the following objects?

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

Answer: A

NEW QUESTION 126
- (Exam Topic 2)
What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

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

D. fw monitor

Answer: D

NEW QUESTION 127
- (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 131
- (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.

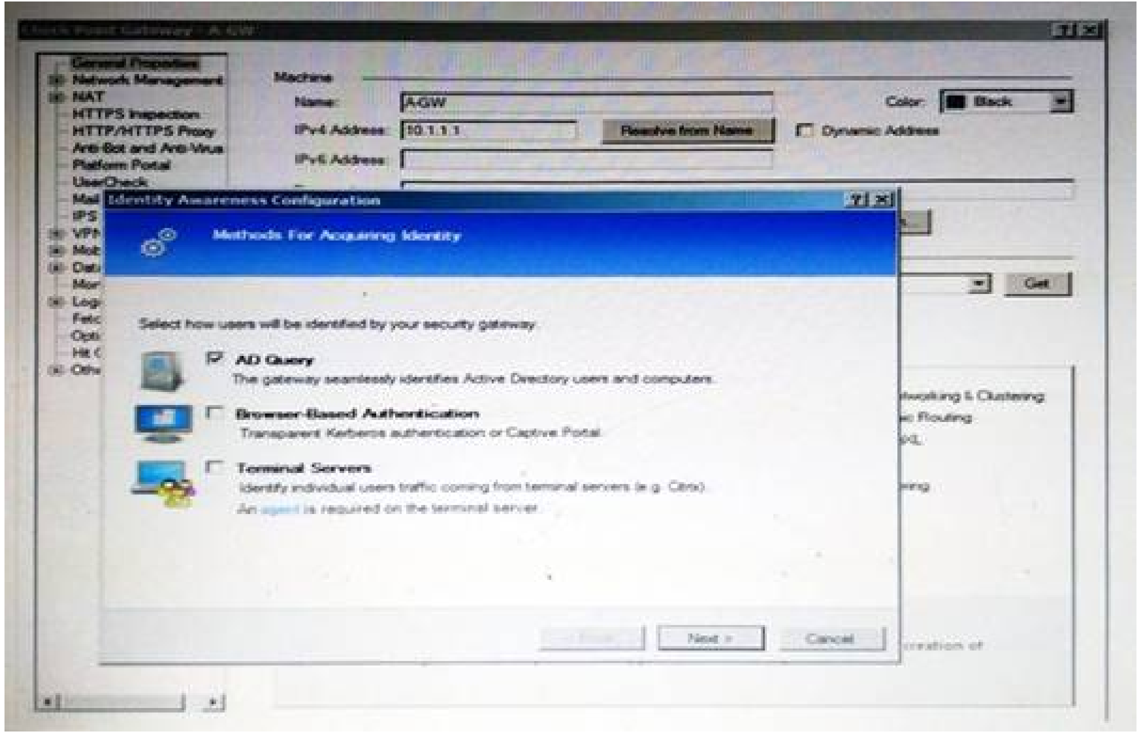
Answer: C

NEW QUESTION 133
- (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 136
- (Exam Topic 2)
On the following picture an administrator configures Identity Awareness:



Machine
Name: AGW
IPv4 Address: 10.1.1.1
Color: Black
□ Dynamic Address

Identity Awareness Configuration
Methods For Acquiring Identity
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 137
- (Exam Topic 2)
You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?

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

Answer: C

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

NEW QUESTION 138
- (Exam Topic 3)
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

A. Threat Emulation
B. Mobile Access
C. Mail Transfer Agent
D. Threat Cloud

Answer: C

NEW QUESTION 140
- (Exam Topic 3)
Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?

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

Answer: C

NEW QUESTION 145
- (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 146
- (Exam Topic 3)
Choose the correct statement regarding Implicit Rules.

A. To edit the Implicit rules you go to: Launch Button > Policy > Global Properties > Firewall.
B. Implied rules are fixed rules that you cannot change.
C. You can directly edit the Implicit rules by double-clicking on a specific Implicit rule.
D. You can edit the Implicit rules but only if requested by Check Point support personnel.

Answer: A

NEW QUESTION 149
- (Exam Topic 3)
How do you configure the Security Policy to provide uses access to the Captive Portal through an external (Internet) interface?

A. Change the gateway settings to allow Captive Portal access via an external interface.
B. No action is necessar
C. This access is available by default.
D. Change the Identity Awareness settings under Global Properties to allow Captive Policy access on all interfaces.
E. Change the Identity Awareness settings under Global Properties to allow Captive Policy access for an external interface.

Answer: A

NEW QUESTION 152
- (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 153
- (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 156
- (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 161
- (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 165
- (Exam Topic 3)
Which command can you use to verify the number of active concurrent connections?

A. fw conn all
B. fw ctl pst pstat
C. show all connections
D. show connections

Answer: B

NEW QUESTION 166
- (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 170
- (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 173
- (Exam Topic 3)
Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?

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

Answer: A

NEW QUESTION 177
- (Exam Topic 3)
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via
e-m ail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?

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

Answer: D

NEW QUESTION 179
- (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 184
- (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 188
- (Exam Topic 3)
Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

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

Answer: A

NEW QUESTION 191
- (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 195
- (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 198
- (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 199
- (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 203
- (Exam Topic 3)
What is the benefit of Manual NAT over Automatic NAT?

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

Answer: C

NEW QUESTION 208
- (Exam Topic 3)
Which tool CANNOT be launched from SmartUpdate R77?

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

Answer: B

NEW QUESTION 212
- (Exam Topic 3)
When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

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

Answer:

C

NEW QUESTION 216
- (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 221
- (Exam Topic 3)
What happens when you run the command: fw sam -J src [Source IP Address]?

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

Answer: A

NEW QUESTION 225
- (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 229
- (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 234
- (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 239
- (Exam Topic 4)
R80.10 management server can manage gateways with which versions installed?

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

Answer: B

NEW QUESTION 243
- (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 248
- (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 249
- (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

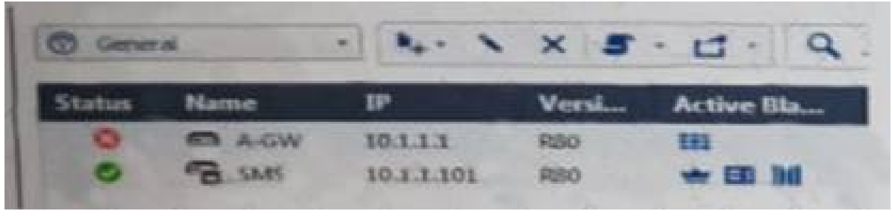
Answer: B

NEW QUESTION 250
- (Exam Topic 4)
What needs to be configured if the NAT property ‘Translate destination on client side’ is not enabled in Global properties?

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

Answer: C

NEW QUESTION 254
- (Exam Topic 4)
What does it mean if Deyra sees the gateway status



Status	Name	IP	Versi...	Active Bla...
●	A-GW	10.1.1.1	R80	
✓	SMS	10.1.1.101	R80	

Choose the BEST answer.

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

Answer: A

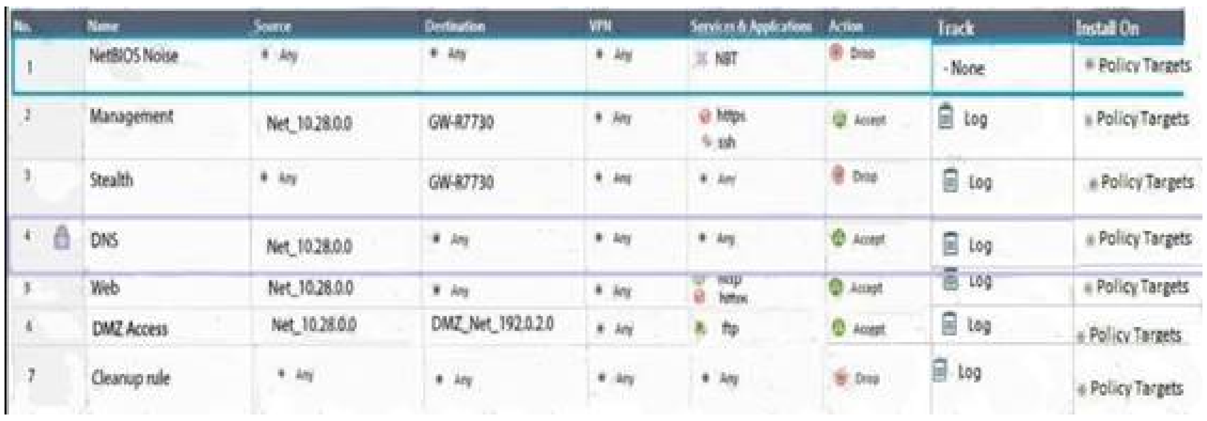
NEW QUESTION 257
- (Exam Topic 4)
The ______ software blade package uses CPU-level and OS-level sandboxing in order to delect and block malware.

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

Answer: B

NEW QUESTION 258
- (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 262
- (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 264
- (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 268
- (Exam Topic 4)
When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

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

Answer: D

NEW QUESTION 269
- (Exam Topic 4)
Using ClusterXL, what statement is true about the Sticky Decision Function?

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

Answer: A

NEW QUESTION 274
- (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 277
- (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 280
- (Exam Topic 4)
John is using Management HA. Which Smartcenter should be connected to for making changes?

A. secondary Smartcenter
B. active Smartcenter
C. connect virtual IP of Smartcenter HA
D. primary Smartcenter

Answer: B

NEW QUESTION 284
- (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 285
- (Exam Topic 4)
Which of the following is an authentication method used for Identity Awareness?

A. SSL
B. Captive Portal
C. PKI
D. RSA

Answer: B

NEW QUESTION 287
- (Exam Topic 4)
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 291
- (Exam Topic 4)
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

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

Answer: C

NEW QUESTION 296
- (Exam Topic 4)
Fill in the blank; The position of an Implied rule is manipulated in the _____ window

A. NAT
B. Firewall
C. Global Properties
D. Object Explorer

Answer: C

NEW QUESTION 301
- (Exam Topic 4)
How many sessions can be opened on the Management Server at the same time?

A. Unlimited, One per each licensed Gateway
B. One
C. Unlimited, Multiple per administrator
D. Unlimited, One per administrator

Answer: D

NEW QUESTION 306
- (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 309
- (Exam Topic 4)
What are the three components for Check Point Capsule?

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

Answer: D

NEW QUESTION 313
- (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 318
- (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 319
- (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 323
- (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 328
- (Exam Topic 4)
Which of the following is the most secure means of authentication?

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

Answer: B

NEW QUESTION 329
- (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 333
......