156-215.80.275q

Number: 156-215.80
Passing Score: 800
Time Limit: 120 min

156-215.80

Check Point Certified Security Administrator R80

Exam A

QUESTION 1

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house R80 Management to the other administrators in ABC Corp.
How will you describe the new "Publish" button in R80 Management Console?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 3
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

QUESTION 4
Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 5
Which of the following is **NOT** a component of a Distinguished Name?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Distinguished Name Components
CN=common name, OU=organizational unit, O=organization, L=locality, ST=state or province, C=country name
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/71950

QUESTION 6
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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*

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/71950

QUESTION 7
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 issues. Change logging storage options on the logging server or Security Management Server properties and install database.
B. Data Awareness is not enabled.

C. Identity Awareness is not enabled.
D. Logs are arriving from Pre-R80 gateways.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 8
What is the order of NAT priorities?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The order of NAT priorities is:
1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/6724.htm#o6919

QUESTION 9
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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
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

QUESTION 10
Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

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

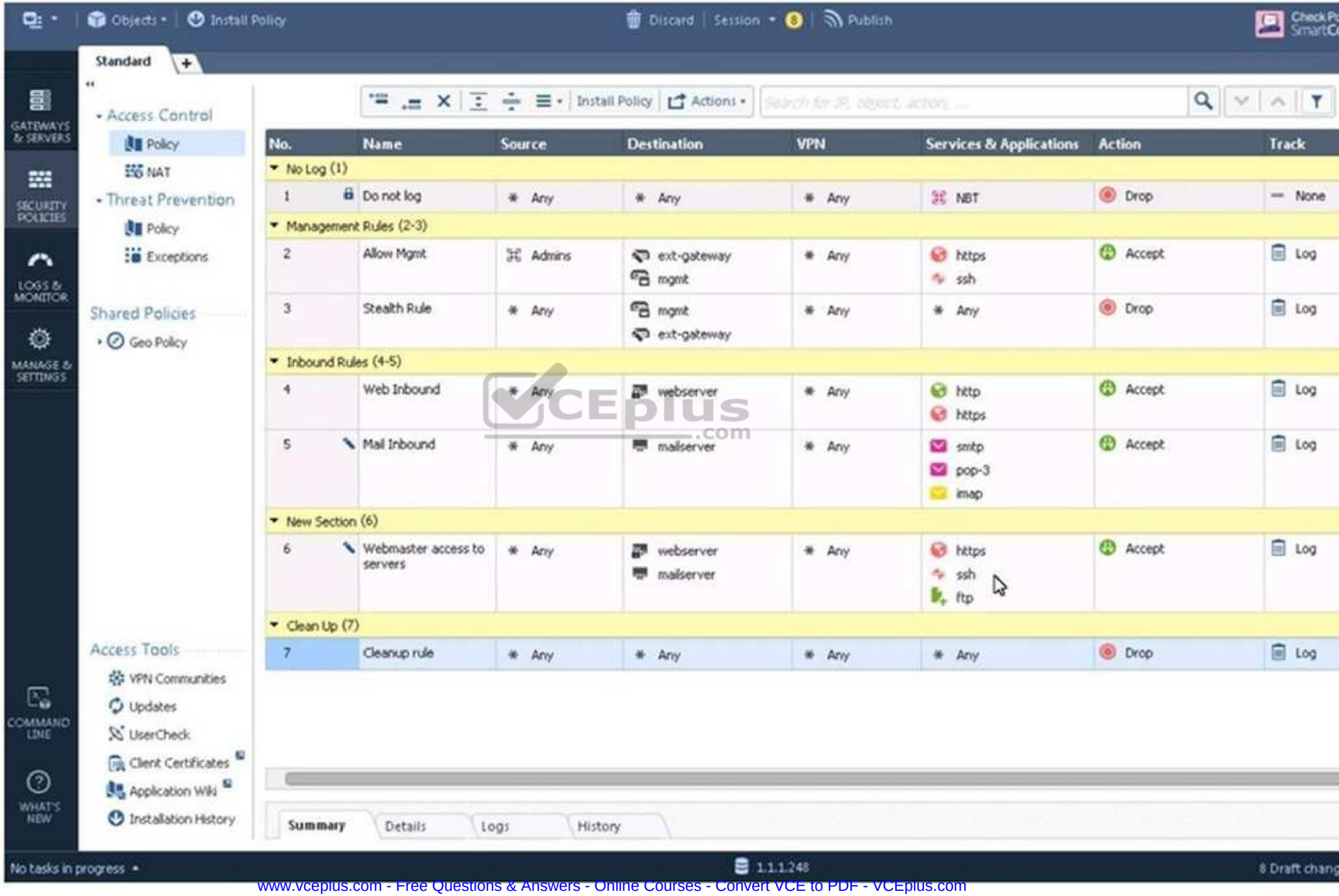
Correct Answer: D
Section: (none)
Explanation

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

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

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm#o73091

QUESTION 11
Examine the following Rule Base.

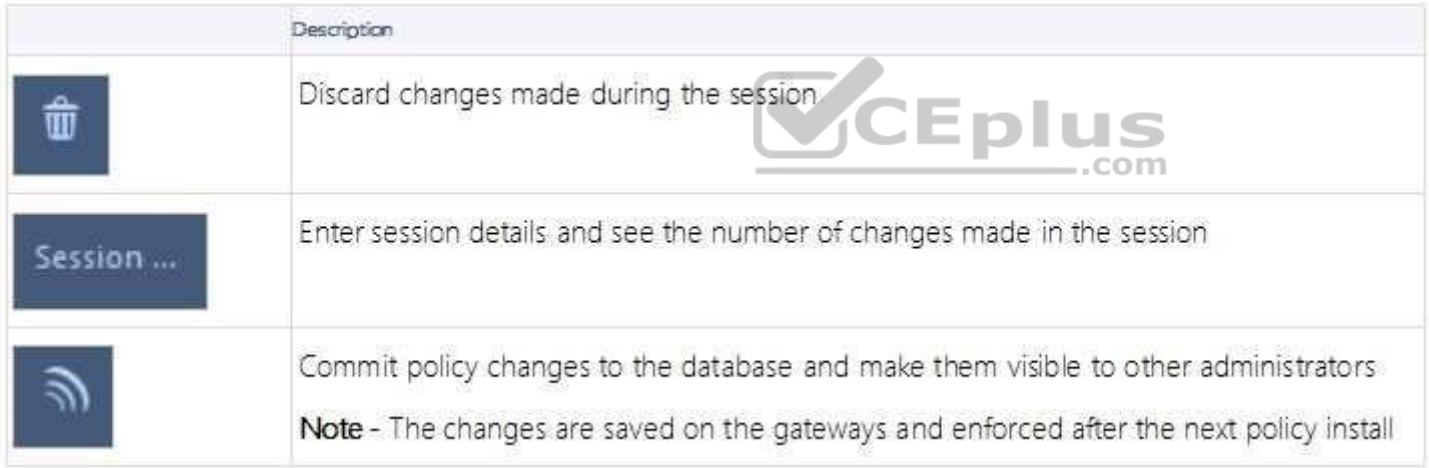


What can we infer about the recent changes made to the Rule Base?

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

Correct Answer: D
Section: (none)
Explanation

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



Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/117948

QUESTION 12
ALPHA 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.

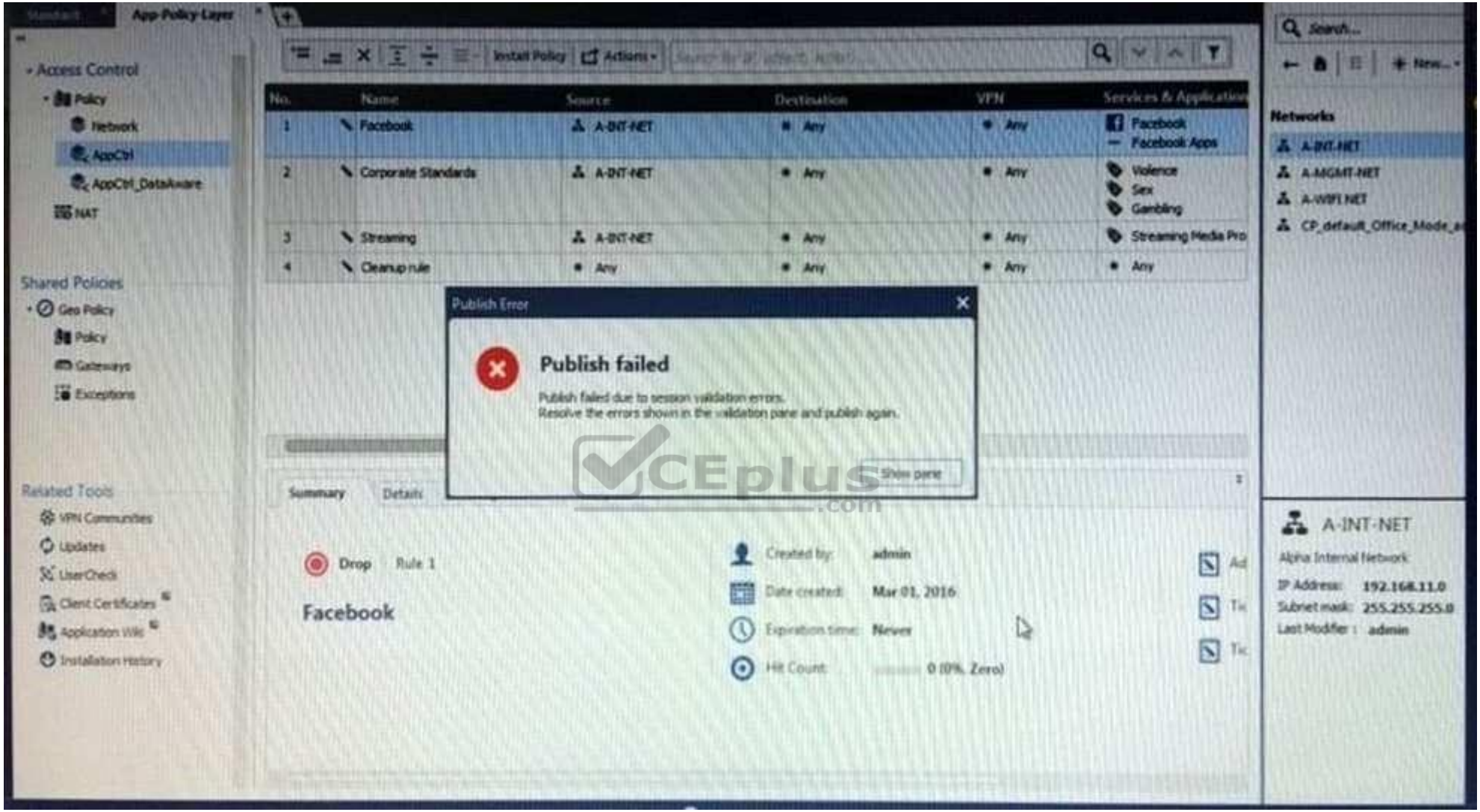
C. The Network address of his computer is in the blocked hosts.
D. The IP address of his computer is not in the allowed hosts.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
There is a lock on top left side of the screen. B is the logical answer.

QUESTION 13

Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.

Where can the administrator check for more information on these errors?



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

D. The Policies section in SmartConsole

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 14
You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Harriet wants to protect sensitive information from intentional loss when users browse to a specific URL: https://personal.mymail.com, which blade will she enable to achieve her goal?

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

Correct Answer: A
Section: (none)
Explanation

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

Reference: https://www.checkpoint.com/downloads/product-related/datasheets/DLP-software-blade-datasheet.pdf

QUESTION 16
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

QUESTION 17
Which of the following is **NOT** a license activation method?

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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 18
Which policy type has its own Exceptions section?

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

Correct Answer: A
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_ThreatPrevention_WebAdmin/82209.htm#o97030

QUESTION 19
By default, which port does the WebUI listen on?

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

Correct Answer: C
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_Gaia_IUG/html_frameset.htm?topic=documents/R80/CP_R80_Gaia_IUG/132120

QUESTION 20
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. Security Gateway

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm

QUESTION 21
Which options are given on features, when editing a Role on Gaia Platform?

A. Read/Write, Read Only
B. Read/Write, Read only, None
C. Read/Write, None
D. Read Only, None

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (read-only) access to other features, and no access to other features.

You can also specify which access mechanisms (WebUI or the CLI) are available to the user.

Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

- **adminRole -** Gives the user read/write access to all features.
- **monitorRole-** Gives the user read-only access to all features. You cannot delete or change the predefined roles.

Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/75930

QUESTION 22

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?HashKey=1479584563_6f823c8ea1514609148aa4fec5425db2&xtn=.pdf

QUESTION 23
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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	

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit_doGoviewsolutiondetails=&solutionid=sk91400

QUESTION 24
With which command can you view the running configuration of Gaia-based system.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which of the following is TRUE regarding Gaia command line?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

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

Correct Answer: A
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 27
Which one of the following is the preferred licensing model? Select the Best answer.

A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.

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

Correct Answer: B
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/13128.htm#o13527

QUESTION 28
Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
B. One machine
C. Two machines
D. Three machines

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
One for Security Management Server and the other one for the Security Gateway.

QUESTION 29

Fill in the blank: A new license should be generated and installed in all of the following situations **EXCEPT** when _____ .

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 30
What is the default shell for the command line interface?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The default shell of the CLI is called `clish`
`Reference:` https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm

QUESTION 31
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: http://dl3.checkpoint.com/paid/71/How_to_Configure_Client_Authentication.pdf?HashKey=1479692369_23bc7cdfbeb67c147ec7bb882d557fd4&xtn=.pdf

QUESTION 32
Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

A. Auditor
B. Read Only All
C. Super User
D. Full Access

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To create a new permission profile:
1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Permission Profiles**.
2. Click **New Profile**.
   The **New Profile** window opens.
3. Enter a unique name for the profile.
4. Select a profile type:
▪ **Read/Write All** - Administrators can make changes

▪ **Auditor (Read Only All)** - Administrators can see information but cannot make changes ▪
Customized - Configure custom settings
5. Click **OK**.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265

QUESTION 33
Packages and licenses are loaded from all of these sources **EXCEPT**

A. Download Center Web site
B. UserUpdate
C. User Center
D. Check Point DVD

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Packages and licenses are loaded into these repositories from several sources:
▪ the Download Center web site (packages)
▪ the Check Point DVD (packages) ▪ the User Center (licenses) ▪ by importing a file (packages and licenses) ▪ by running the `cplic` command line
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/13128.htm

QUESTION 34
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/smb/help/utm1/8.2/7080.htm

QUESTION 35
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.

Correct Answer: B

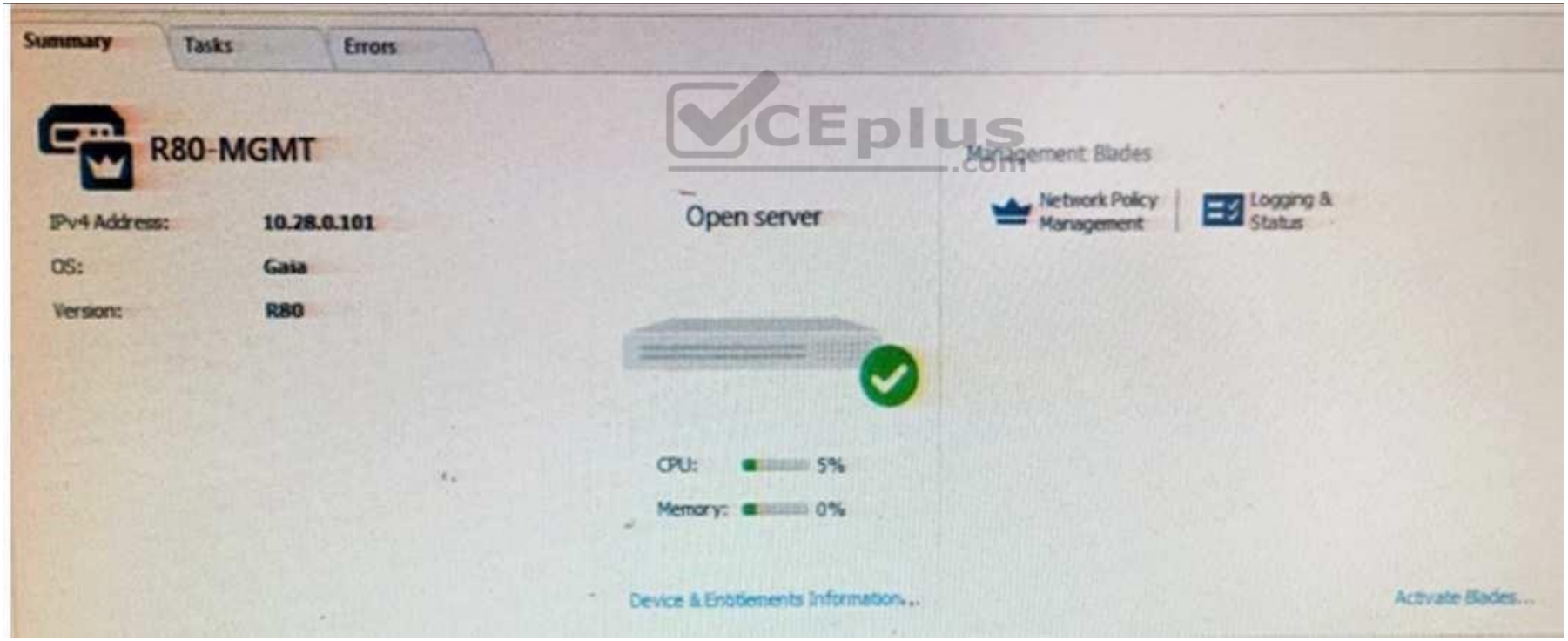
Section: (none)
Explanation

Explanation/Reference:
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

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 36
Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the Summary screen as in the screenshot below. What as an 'Open Server'?



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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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).

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/index.html

QUESTION 37
Choose what BEST describes the Policy Layer Traffic Inspection.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.checkpoint.com/thread/1092

QUESTION 38
What are the three conflict resolution rules in the Threat Prevention Policy Layers?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 39
What does the “unknown” SIC status shown on SmartConsole mean?

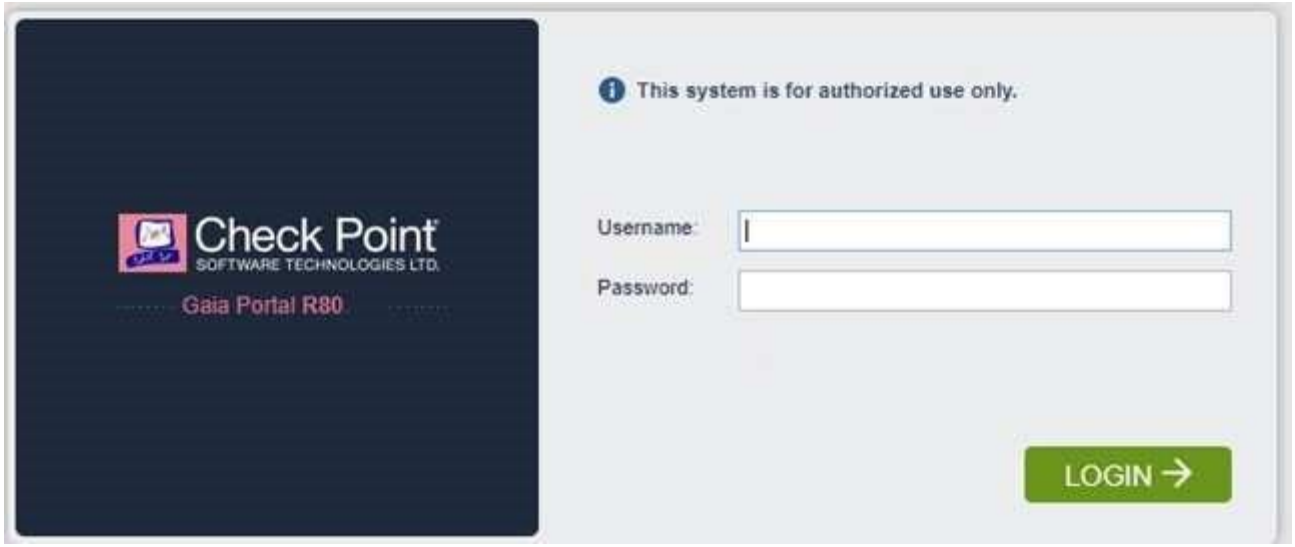
A. The SMS can contact the Security Gateway but cannot establish Secure Internal Communication.
B. SIC activation key requires a reset.
C. The SIC activation key is not known by any administrator.
D. There is no connection between the Security Gateway and SMS.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 and 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.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/118037

QUESTION 40
Kofi, the administrator of the ALPHA Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In Clish
A. Connect to command line on Security Gateway / *each* Cluster member.
B. Log in to Clish.
C. Set the desired port (e.g., port 4434):**HostName> set web ssl-port <Port_Number>** D. Save the changes:
HostName> save config
E. Verify that the configuration was saved:
[Expert@HostName]# grep 'httpd:ssl_port' /config/db/initial Reference:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482

QUESTION 41
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____ .

A. User Directory
B. Captive Portal and Transparent Kerberos Authentication
C. Captive Portal
D. UserCheck

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To enable Identity Awareness:
1. Log in to SmartDashboard.
2. From the Network Objects tree, expand the **Check Point** branch.
3. Double-click the Security Gateway on which to enable Identity Awareness.
4. In the Software Blades section, select **Identity Awareness** on the Network Security tab.
   The **Identity Awareness** Configuration wizard opens.
5. 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.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62050.htm

QUESTION 42
Which default user has full read/write access?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Fill in the blanks: 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Fill in the blank: To build an effective Security Policy, use a _____ and _____ rule.

A. Cleanup; stealth
B. Stealth; implicit

C. Cleanup; default
D. Implicit; explicit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101878

QUESTION 48
The following graphic shows:

Logs | New Tab

Last 7 Days • src:10.1.1.202

Showing first 50 results (464 ms) out of 1,318 results

Time	B...	I...	Origin	A...	Source	Source User N...	Destination	Service	Rule	Policy...	User	Source Machine...	Descript
Today, 5:30:27 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:30:26 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:36 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:35 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:35 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:34 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:23 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:22 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:00 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:59 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:48 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:47 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:35 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:34 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:23 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:22 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:02 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:01 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:51 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:50 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:23 AM			A-GW		10.1.1.202		10.1.1.255	nbdatagram	1	Standard			
Today, 5:20:18 AM			A-GW		10.1.1.202		10.1.1.255	nbname	1	Standard			
Today, 5:09:26 AM			A-GW		10.1.1.202		10.1.1.255	nbdatagram	1	Standard			
Today, 5:03:58 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:57 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:52 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:51 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197&anchor=o129934

QUESTION 50
Fill in the blank: The command _____ provides the most complete restoration of a R80 configuration.

A. `upgrade_import`
B. `cpconfig`
C. `fwm dbimport -p <export file>`
D. `cpinfo -recover`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
(Should be "migrate import")
"migrate import" Restores backed up configuration for R80 version, in previous versions the command was " `upgrade_import` ".
Reference: http://dl3.checkpoint.com/paid/08/08586e2852acc054809517b267402a35/CP_R80_Gaia_InstallationAndUpgradeGuide.pdf?HashKey=1479700086_4553ede4b53a7882cd8052eed7c347be&xtn=.pdf

QUESTION 51
The Gaia operating system supports which routing protocols?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Advanced Routing Suite
The Advanced Routing Suite CLI is available as part of the Advanced Networking Software Blade.

For organizations looking to implement scalable, fault-tolerant, secure networks, the Advanced Networking blade enables them to run industry-standard dynamic routing protocols including BGP, OSPF, RIPv1, and RIPv2 on security gateways. OSPF, RIPv1, and RIPv2 enable dynamic routing over a single autonomous system—like a single department, company, or service provider—to avoid network failures. BGP provides dynamic routing support across more complex networks involving multiple autonomous systems—such as when a company uses two service providers or divides a network into multiple areas with different administrators responsible for the performance of each.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecurePlatform_AdvancedRouting_WebAdmin/html_frameset.htm

QUESTION 52
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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:
1. Enter this URL in your browser: https://<Gaia IP address>
2. Enter your user name and password.

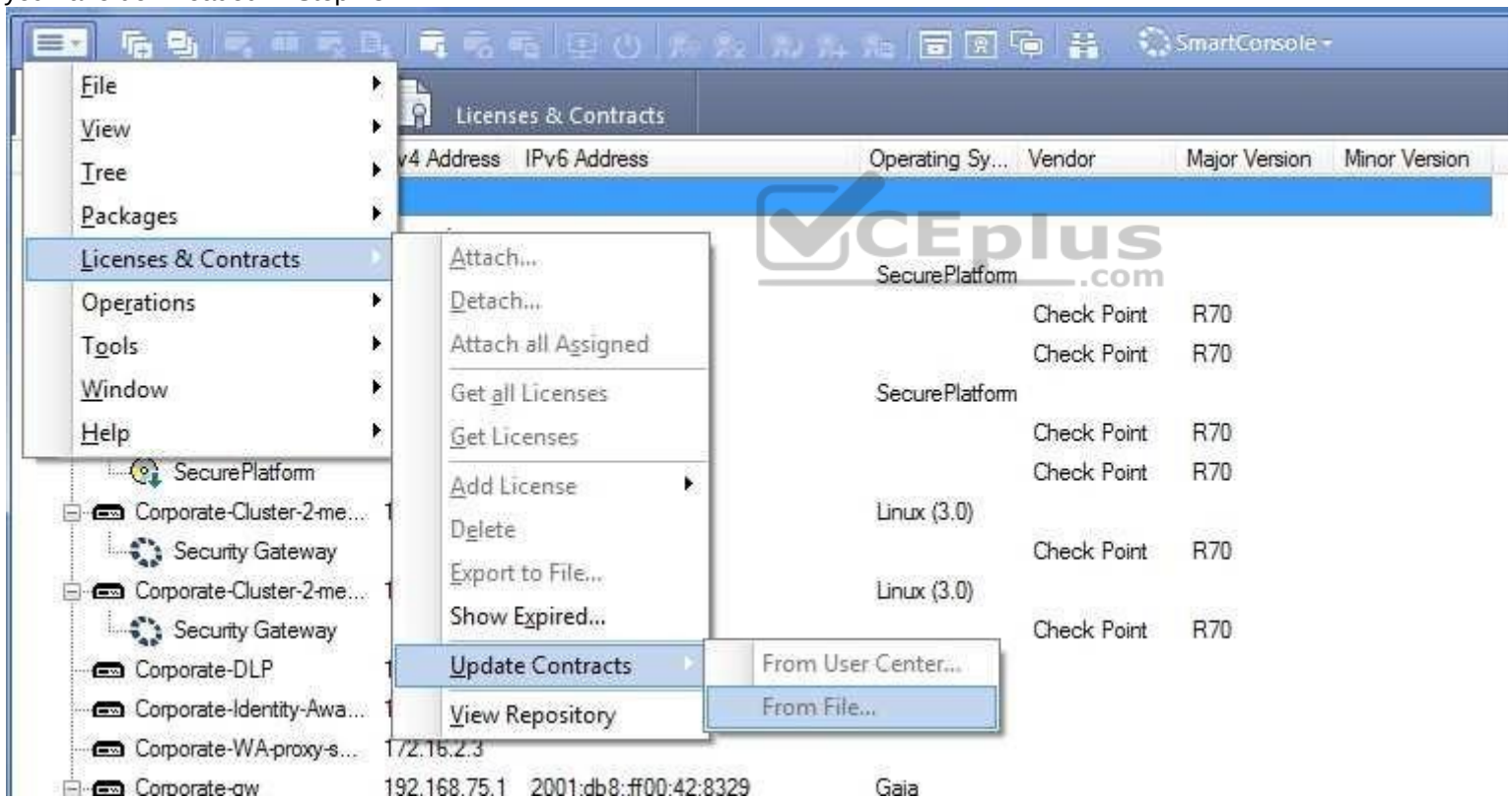
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/75930

QUESTION 53
Which application should you use to install a contract file?

A. SmartView Monitor
B. WebUI

C. SmartUpdate
D. SmartProvisioning

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
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.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk33089

QUESTION 54
Which feature is NOT provided by all Check Point Mobile Access solutions?
A. Support for IPv6
B. Granular access control
C. Strong user authentication
D. Secure connectivity

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Types of Solutions
All of Check Point's Remote Access solutions provide:
▪ Enterprise-grade, secure connectivity to corporate resources.
▪ Strong user authentication. ▪
Granular access control.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/83586.htm

QUESTION 55
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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://www.checkpoint.com/products-solutions/zero-day-protection/

QUESTION 56
Fill in the blank: Each cluster has _____ interfaces.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

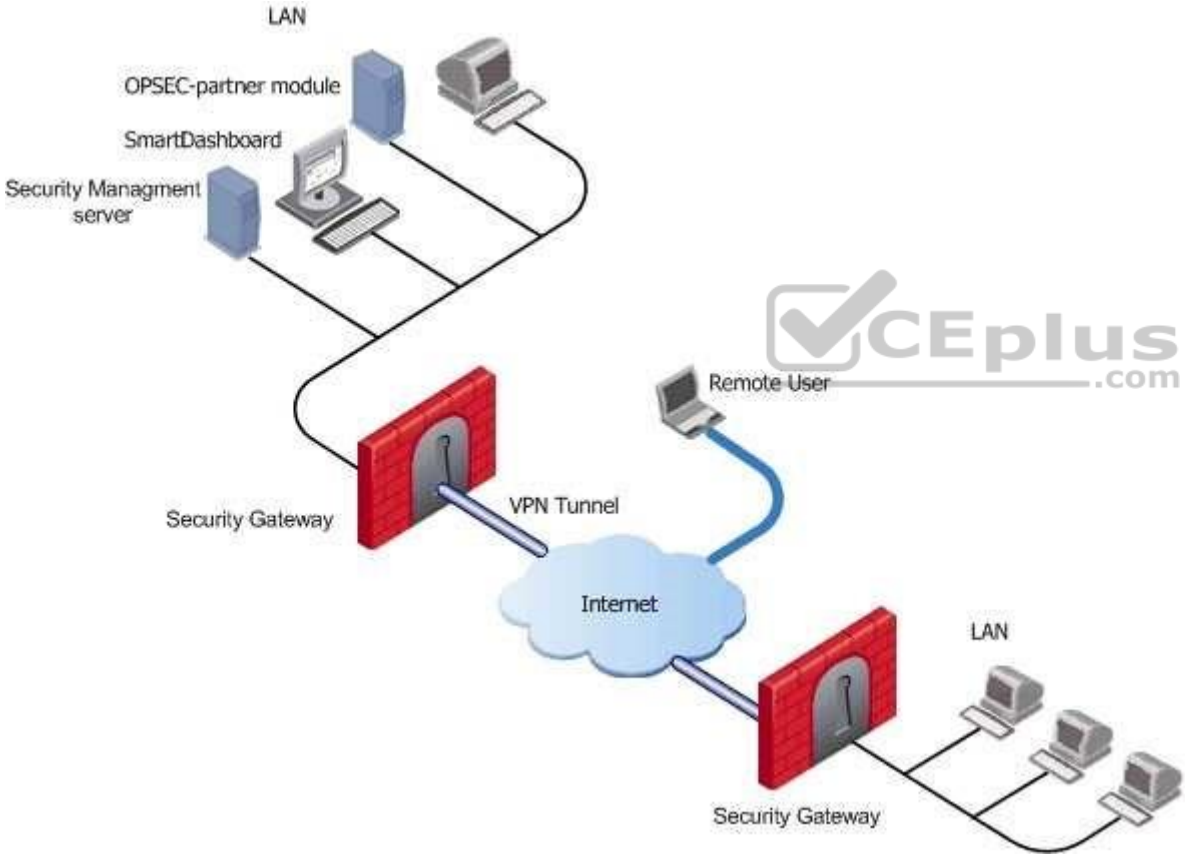
QUESTION 57
What are the three essential components of the Check Point Security Management Architecture?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:
Deployments
Basic deployments:
- Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.
- Distributed deployment - Security Gateway and the Security Management server are installed on different machines.



Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.
You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.

The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer. There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/118037

QUESTION 58
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

Correct Answer: D
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/6724.htm

QUESTION 59

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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) **Explanation :**
Symptoms

- SmartDashboard fails to connect to the Security Management server.

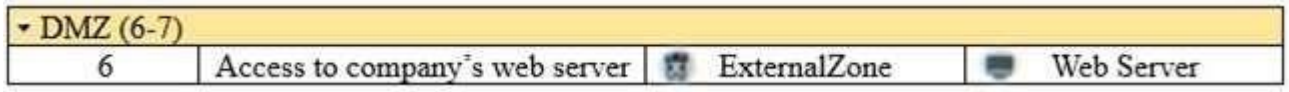
```
APP          PID     STAT  #START  START_TIME          MON  COMMAND
CPVIEWD      3075    E     1       [16:26:54] 5/5/2016 N    cpviewd
CPD          0       T     1       [17:15:57] 6/5/2016 N    cpd
FWD          21752   E     1       [17:15:51] 6/5/2016 N    fwd -n
CPM          0       T     1       [15:32:23] 6/5/2016 N    /opt/CPsuite-R80/fw1/scripts/cpm.sh -s
FWM          0       T     1       [17:15:45] 6/5/2016 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_inde
SMARTLOG_    SERVER  7977  E  1    [16:32:53] 5/5/2016 N    /opt/CPSmartLog-R80/smartlog_serve
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] 5/5/2016 N    cpstat_monitor
```

1. Verify if the FWM process is running. To do this, run the command:
[Expert@HostName:0]# ps -aux | grep fwm
2. 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"

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk12120

QUESTION 60
What does ExternalZone represent in the presented rule?



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.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Configuring Interfaces
Configure the Security Gateway 80 interfaces in the **Interfaces** tab in the Security Gateway window.
To configure the interfaces:
1. From the **Devices** window, double-click the Security Gateway 80.
The **Security Gateway** window opens.
2. Select the **Interfaces** tab.
3. Select **Use the following settings**. The interface settings open.
4. Select the interface and click **Edit**.
The **Edit** window opens.
5. From the IP Assignment section, configure the IP address of the interface:
1. Select **Static IP**.
2. Enter the IP address and subnet mask for the interface.
6. 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.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartProvisioning_WebAdmin/16741.htm

QUESTION 61
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

Correct Answer: C
Section: (none)
Explanation

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

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

QUESTION 62

What are the two high availability modes?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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**

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm#o7363

QUESTION 63
Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Suspicious Activity Rules Solution
Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).
The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an **Install Policy** operation
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartViewMonitor_AdminGuide/17670.htm

QUESTION 64
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

Reference: https://www.checkpoint.com/products/ips-software-blade/

QUESTION 65
What is the purpose of Captive Portal?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 66
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To enable Identity Awareness:
1. Log in to SmartDashboard.
2. From the Network Objects tree, expand the **Check Point** branch.
3. Double-click the Security Gateway on which to enable Identity Awareness.
4. In the Software Blades section, select **Identity Awareness** on the Network Security tab.
   The **Identity Awareness** Configuration wizard opens.
5. 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.

6. 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 **all** of the domain controllers in the organization's Active Directory.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62050.htm

QUESTION 67
Which policy type is used to enforce bandwidth and traffic control rules?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Check Point's QoS Solution
QoS is a policy-based QoS management solution from Check Point Software Technologies Ltd., satisfies your needs for a bandwidth management solution. QoS is a unique, software-only based application that manages traffic end-to-end across networks, by distributing enforcement throughout network hardware and software. Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_QoS_AdminGuide/index.html

QUESTION 68
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/118981

QUESTION 70
Which Check Point software blade provides protection from zero-day and undiscovered threats?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73101.htm

QUESTION 72
Look at the following screenshot and select the BEST answer.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Fill in the blanks: A security Policy is created in _____ , stored in the _____ , and Distributed to the various _____ .
A. Rule base, Security Management Server, Security Gateways B.
SmartConsole, Security Gateway, Security Management Servers
C. SmartConsole, Security Management Server, Security Gateways
D. The Check Point database, SmartConsole, Security Gateways

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Look at the screenshot below. What CLISH command provides this output?

```
#
# Configuration of R80-MGMT
# Language version: 13.0v1
#
# Exported by admin on Fri Apr 22 13:22:45 2016
#
set installer policy periodically-self-update on
set installer policy send-cpuse-data off
set installer policy self-test auto-rollback off
set installer policy self-test install-policy off
set installer policy self-test network-link-up off
set installer policy self-test start-processes on
set arp table cache-size 4096
set arp table validity-timeout 60
set arp announce 2
set message banner on

set message motd off

set message caption off
set core-dump enable
set core-dump total 1000
set core-dump per_process 2
set clienv debug 0
set clienv echo-cmd off
-- More --
```

A. show configuration all
B. show confd configuration
C. show confd configuration all
D. `show configuration`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To see the latest configuration settings, run:

```
show configuration
```

This example shows part of the configuration settings as last saved to a CLI script:

```
mem103> show configuration
#
# Configuration of mem103
# Language version: 10.0v1
#
# Exported by admin on Mon Mar 19 15:06:22 2012
#
set hostname mem103
set timezone Asia / Jerusalem
set password-controls min-password-length 6
set password-controls complexity 2
set password-controls palindrome-check true
set password-controls history-checking true
set password-controls history-length 10
set password-controls password-expiration never
set ntp active off
set router-id 6.6.6.103
set ipv6-state off
set snmp agent off
set snmp agent-version any
set snmp community public read-only
set snmp traps trap authorizationError disable
set snmp traps trap coldStart disable
set snmp traps trap configurationChange disable
```


Reference: http://dl3.checkpoint.com/paid/0c/0caa9c0daa67e0c1f2af3dd06790bc81/CP_R77_Gaia_AdminGuide.pdf?HashKey=1479835768_76058f0fc4209e38bc801cd58a85d7c5&xtn=.pdf

QUESTION 75
Which authentication scheme requires a user to possess a token?

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

Correct Answer: B
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityGatewayTech_WebAdmin/6721.htm

QUESTION 76
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Implied Rules are configured only on Global Properties.

QUESTION 77
The most important part of a site-to-site VPN deployment is the _____ .
A. Internet
B. Remote users
C. Encrypted VPN tunnel
D. VPN gateways

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Site to Site VPN

The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time. Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92709.htm

QUESTION 78
R80 Security Management Server can be installed on which of the following operating systems?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
R80 can be installed only on GAIA OS.

Supported Check Point Installations All R80 servers are supported on the Gaia Operating System:
• Security Management Server
• Multi-Domain Security Management Server
• Log Server
• Multi-Domain Log Server
• SmartEvent Server

Reference: http://dl3.checkpoint.com/paid/1f/1f7e21da67aa992954aa12a0a84e53a8/CP_R80_ReleaseNotes.pdf?

HashKey=1479838085_d6ffcb36c6a3128708b3f6d7bcc4f94e&xtn=.pdf

QUESTION 79
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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`

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902

QUESTION 81
Choose what BEST describes users on Gaia Platform.
A. There is one default user that cannot be deleted.
B. There are two default users and one cannot be deleted.
C. There is one default user that can be deleted.
D. There are two default users that cannot be deleted and one SmartConsole Administrator.

Correct Answer: B

Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73101.htm

QUESTION 82
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`

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 saved.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902

QUESTION 83
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 managed. Consult the R80 Release Notes for more information.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

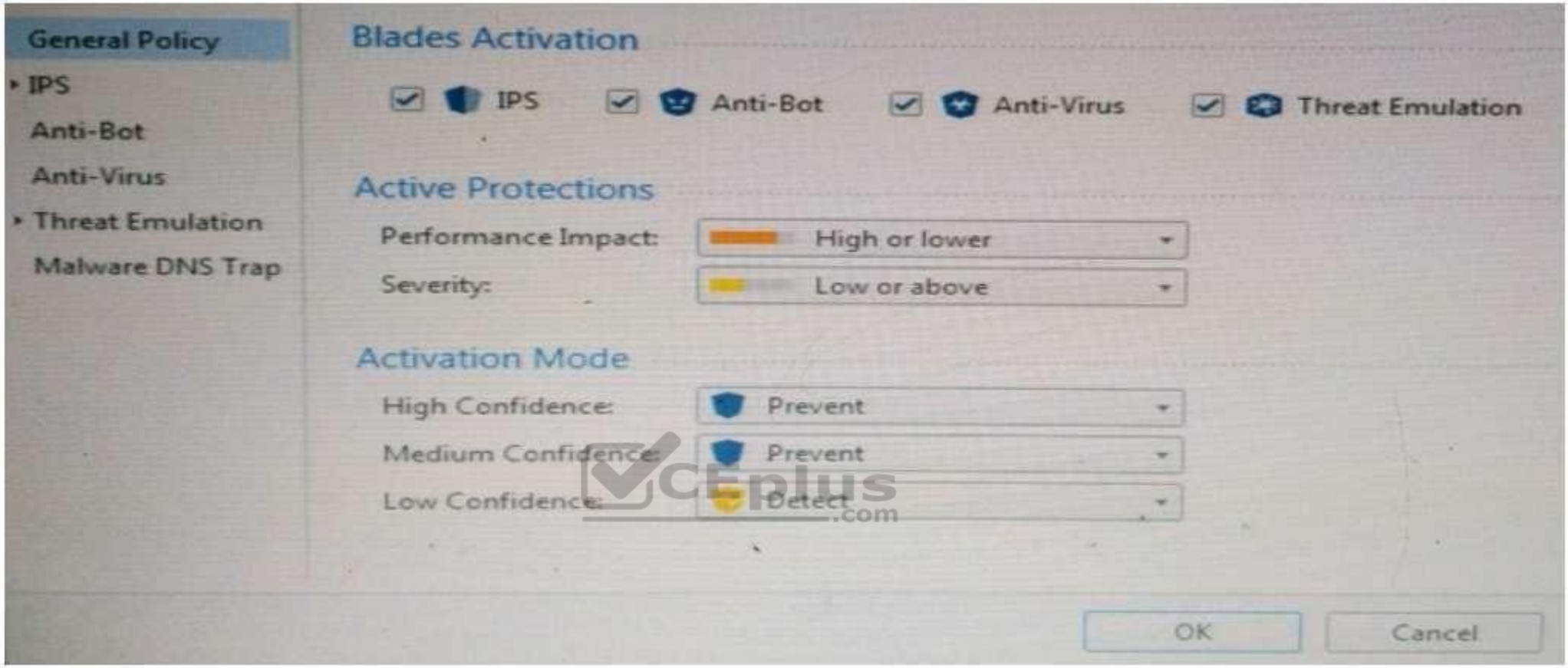
Compatibility with Gateways

R80 Management Servers can manage gateways of these versions:

Release	Version
Security Gateway	R75.20, R75.30, R75.40, R75.45, R75.40VS, R75.46, R75.47, R76 R77, R77.10, R77.20, R77.30
Security Gateway 80	R71.45, R75.20.x
1100 Appliance	R75.20.x, R77.20.x
1200R Appliance	R77.20.x
UTM-1 Edge	7.5.x and higher (Edge-X and Edge-W are not supported)

Reference: http://dl3.checkpoint.com/paid/1f/1f7e21da67aa992954aa12a0a84e53a8/CP_R80_ReleaseNotes.pdf?HashKey=1479838085_d6ffcb36c6a3128708b3f6d7bcc4f94e&xtn=.pdf

QUESTION 84
Provide very wide coverage for all products and protocols, with noticeable performance impact.



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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

QUESTION 86
Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.

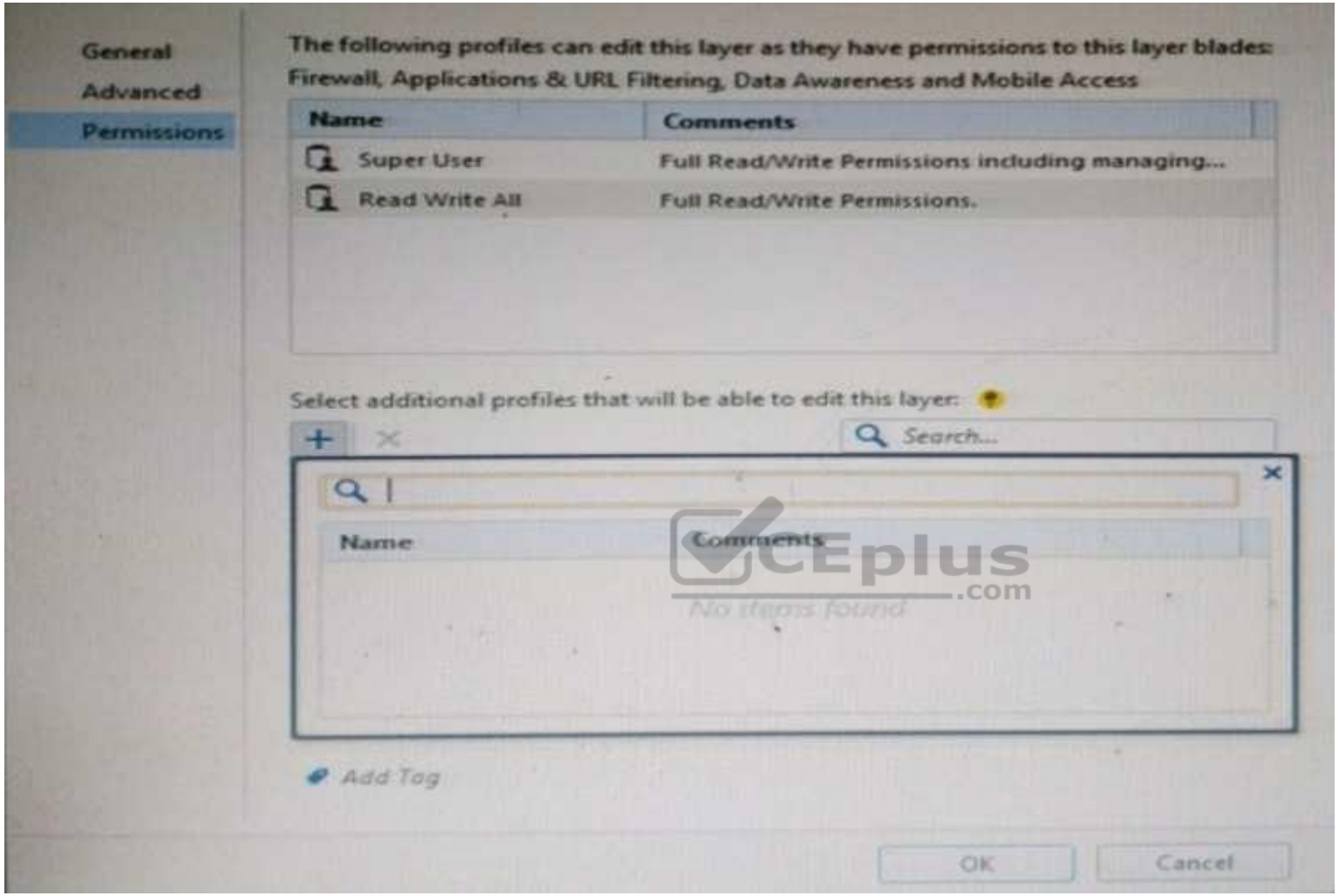
A. Shared policy packages
B. Shared policies
C. Concurrent policy packages
D. Concurrent policies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87

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



A. “Edit layers by Software Blades” is unselected in the Permission Profile B.
There are no permission profiles available and you need to create one first.

C. All permission profiles are in use.

D. “Edit layers by selected profiles in a layer editor” is unselected in the Permission profile.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following is **NOT** an alert option?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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**.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_SmartViewMonitor_AdminGuide/101104.htm

QUESTION 89
Fill in the blanks: A High Availability deployment is referred to as a _____ cluster and a Load Sharing deployment is referred to as a _____ cluster.

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

Correct Answer: D

Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_ClusterXL_WebAdminGuide/7292.htm

QUESTION 90
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/13139

QUESTION 92
Which of the following is NOT a set of Regulatory Requirements related to Information Security?

A. ISO 37001
B. Sarbanes Oxley (SOX)
C. HIPPA
D. PCI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
ISO 37001 - Anti-bribery management systems
Reference: http://www.iso.org/iso/home/standards/management-standards/iso37001.htm

QUESTION 93
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`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Obtaining a Configuration Lock

- `lock database override`
- `unlock database`

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm#o73091

QUESTION 94
Joey is using the computer with IP address 192.168.20.13. He wants to access web page "www.CheckPoint.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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
Fill in the blank: Licenses can be added to the License and Contract repository _____ .

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/13128.htm

QUESTION 96
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

Correct Answer: E
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

QUESTION 97
Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____ .

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents/R80/CP_R80BC_ThreatPrevention/136486

QUESTION 98
Fill in the blank: RADIUS Accounting gets _____ data from requests generated by the accounting client

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
How RADIUS Accounting Works with Identity Awareness
RADIUS Accounting gets identity data from **RADIUS Accounting Requests** generated by the RADIUS accounting client.
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/62050

QUESTION 99
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/131915

QUESTION 100
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://www.checkpoint.com/products/identity-awareness-software-blade/

QUESTION 101
How many users can have read/write access in Gaia at one time?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAiA, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, gateway policy permits access only from Join's desktop which is assigned an IP address 10.0.0.19 via DHCP.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but the limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to move around the organization and continue to have access to the HR Web Server. To make this scenario work, the IT administrator:

1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources.
2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

A. John should install the identity Awareness Agent
B. The firewall admin should install the Security Policy
C. John should lock and unlock the computer

D. Investigate this as a network connectivity issue

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which feature in R77 permits blocking specific IP addresses for a specified time period?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 107
Which of the following statements accurately describes the command `snapshot`?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Anti-Spoofing is typically set up on which object type?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 112
Message digests use which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
When using LDAP as an authentication method for Identity Awareness, the query:

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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 114
Which of the below is the MOST correct process to reset SIC from SmartDashboard?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
You have two rules, ten users, and two user groups in a Security Policy. You create database version 1 for this configuration. You then delete two existing users and add a new user group. You modify one rule and add two new rules to the Rule Base. You save the Security Policy and create database version 2. After a while, you decide to roll back to version 1 to use the Rule Base, but you want to keep your user database. How can you do this?

A. Run `fwm dbexport -l filename`. Restore the database. Then, run `fwm dbimport -l filename` to import the users.
B. Run `fwm_dbexport` to export the user database. Select restore the entire database in the Database Revision screen. Then, run `fwm_dbimport`.
C. Restore the entire database, except the user database, and then create the new user and user group.
D. Restore the entire database, except the user database.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor

C. SmartView Tracker, CPINFO, SmartUpdate
D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 124
What is Consolidation Policy?

A. The collective name of the Security Policy, Address Translation, and IPS Policies.
B. The specific Policy written in SmartDashboard to configure which log data is stored in the SmartReporter database.
C. The collective name of the logs generated by SmartReporter.
D. A global Policy used to share a common enforcement policy for multiple Security Gateways.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Where do you verify that UserDirectory is enabled?

A. Verify that **Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways** is checked
B. Verify that **Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways** is checked.
C. Verify that **Security Gateway > General Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP)** for Security Gateways is checked.
D. Verify that **Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways** is checked.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
What is the Manual Client Authentication TELNET port?
A. 23
B. 264
C. 900
D. 259

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.

To make this scenario work, the IT administrator must:

1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action. 4) Install policy.
Ms McHanry tries to access the resource but is unable. What should she do?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
How many packets does the IKE exchange use for Phase 1 Main Mode?
A. 12
B. 1
C. 3
D. 6

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
What is also referred to as **Dynamic NAT**?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the **Install On** check box. What should you look for?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 136
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

A. 3DES and MD5
B. Certificates and IPsec
C. Certificates and pre-shared secret
D. IPsec and VPN Domains

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Where does the security administrator activate Identity Awareness within SmartDashboard?

A. **Gateway Object > General Properties**
B. **Security Management Server > Identity Awareness**
C. **Policy > Global Properties > Identity Awareness**
D. **LDAP Server Object > General Properties**

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
QUESTION 141
While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?

1) Select **Active Mode** tab in SmartView Tracker.
2) Select **Tools > Block Intruder**.
3) Select **Log Viewing** tab in SmartView Tracker.
4) Set **Blocking Timeout** value to 60 minutes.
5) Highlight connection that should be blocked.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 146
What port is used for communication to the User Center with SmartUpdate?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
How do you configure an alert in SmartView Monitor?

A. An alert cannot be configured in SmartView Monitor.
B. By choosing the Gateway, and **Configure Thresholds**.
C. By right-clicking on the Gateway, and selecting **Properties**.
D. By right-clicking on the Gateway, and selecting **System Information**.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Which of these attributes would be critical for a site-to-site VPN?

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

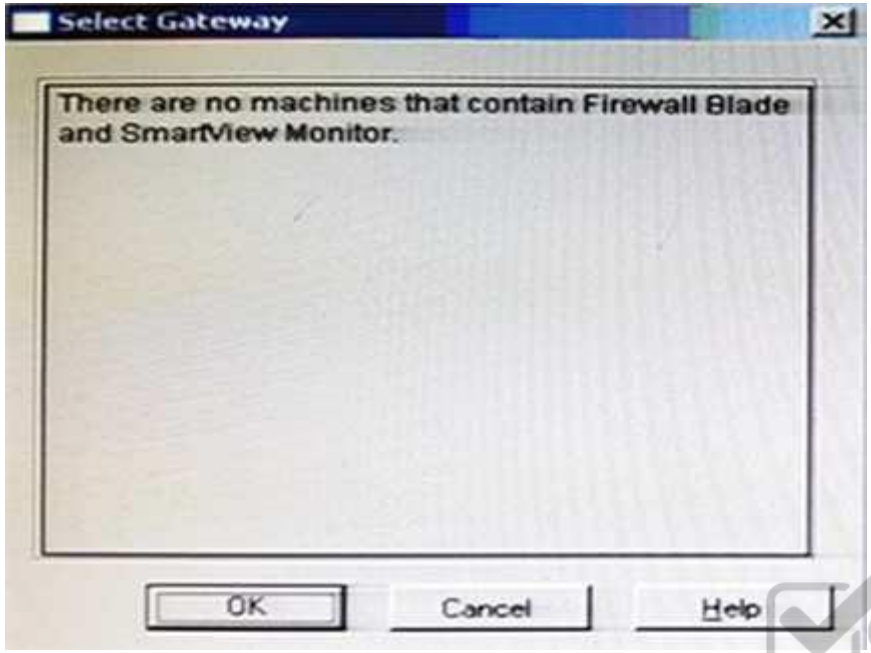
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.

Unfortunately, you get the message:
"There are no machines that contain Firewall Blade and SmartView Monitor".

What should you do to analyze the packet size distribution of your traffic? Give the BEST answer.



A. Purchase the SmartView Monitor license for your Security Management Server.
B. Enable Monitoring on your Security Management Server.
C. Purchase the SmartView Monitor license for your Security Gateway.
D. Enable Monitoring on your Security Gateway.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners. Which SmartConsole application should you use to confirm your suspicious?

A. SmartDashboard

B. SmartUpdate
C. SmartView Status
D. SmartView Tracker

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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 necessary. This access is available by default.
C. Change the Identity Awareness settings under Global Properties to allow Captive Policy access on all interfaces.
D. Change the Identity Awareness settings under Global Properties to allow Captive Policy access for an external interface.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154

The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the following should you remember?

A. You can only use the rule for Telnet, FTP, SMPT, and rlogin services.
B. The Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.
C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
D. You can limit the authentication attempts in the **User Properties' Authentication** tab.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.
John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his desktop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.
To make this scenario work, the IT administrator:
1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location. 3) Changes from static IP address to DHCP for the client PC.
What should John request when he cannot access the web server from his laptop?

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

Correct Answer: C

Section: (none)
Explanation
Explanation/Reference:

QUESTION 158
Review the rules. Assume domain UDP is enabled in the implied rules.

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

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which component functions as the Internal Certificate Authority for R77?

A. Security Gateway
B. Management Server
C. Policy Server
D. SmartLSM

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

A. Source Address
B. Destination Address
C. TCP Acknowledgment Number
D. Source Port

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/92711.htm

QUESTION 161
When defining QoS global properties, which option below is not valid?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_QoS_AdminGuide/14871.htm

QUESTION 162
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109

QUESTION 163
How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

A. Install appliance TE250X on SpanPort on LAN switch in MTA mode
B. Install appliance TE250X in standalone mode and setup MTA
C. You can utilize only Check Point Cloud Services for this scenario
D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://dl3.checkpoint.com/paid/f2/f2faf02dba06acad8cc4c57833593df6/CP_TE100X_TE250X_Appliance_GettingStartedGuide.pdf?HashKey=1517091196_a292abdde351bbdb4b3d28e82654b240&xtn=.pdf

QUESTION 164
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

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

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEvent_AdminGuide/17401.htm

QUESTION 165
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf?HashKey=1517091458_be29bd4732d8d22283df32ccaaffc482&xtn=.pdf

QUESTION 166
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/latest/APIs/index.html#cli/add-host~v1.1

QUESTION 167

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/products-solutions/zero-day-protection/

QUESTION 168
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
What is the command to see cluster status in cli expert mode?

A. fw ctl stat
B. clusterXL stat
C. clusterXL statusD. cphaprob stat

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 170
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/120829

QUESTION 171
If the first packet of an UDP session is rejected by a security policy, what does the firewall send to the client?

A. Nothing
B. TCP FIN
C. TCP RST
D. ICMP unreachable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

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

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

QUESTION 175
Which of the following is NOT an attribute of packer acceleration?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92711.htm

QUESTION 176
Which is a suitable command to check whether Drop Templates are activated or not?

A. fw ctl get int activate_drop_templates
B. fwaccel stat
C. fwaccel stats
D. fw ctl templates –d

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk71200

QUESTION 177
Please choose correct command syntax to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

A. host name myHost12 ip-address 10.50.23.90
B. mgmt add host name ip-address 10.50.23.90
C. add host name emailserver1 ip-address 10.50.23.90

D. mgmt add host name emailserver1 ip-address 10.50.23.90

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97443

QUESTION 179
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

Correct Answer: A
Section: (none)
Explanation QUESTION
180
What command would show the API server status?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
How Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VPN. Capsule Workspace provides a Desktop with usable applications
B. Capsule Workspace can provide access to any application
C. Capsule Connect provides Business data isolation
D. Capsule Connect does not require an installed application at client

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

A. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. Time object to a rule to make the rule active only during specified times.

Explanation/Reference:

D. Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://dl3.checkpoint.com/paid/1f/1f850d1640792cf885336cc6ae8b2743/CP_R80_ReleaseNotes.pdf?HashKey=1517092603_dd917544d92dccc060e5b25d28a46f79&xtn=.pdf

QUESTION 183
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/products-solutions/mobile-security/check-point-capsule/

QUESTION 184
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

Correct Answer: B
Section: (none)
Explanation
QUESTION 185

What is true about the IPS-Blade?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
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 task. Check Point will make use of the newly installed CPU and Cores
D. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

A. Any size

Explanation/Reference:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/120829

QUESTION 188
Which firewall daemon is responsible for the FW CLI commands?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 189
If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

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

Correct Answer: A
Section: (none)

Explanation

QUESTION 190

Using R80 Smart Console, what does a “pencil icon” in a rule mean?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R80/APIs/#introduction

QUESTION 192

Session unique identifiers are passed to the web api using which http header option?

Explanation/Reference:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
What is the main difference between Threat Extraction and Threat Emulation?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 194
Which path below is available only when CoreXL is enabled?

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

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 195
Which of the following describes how Threat Extraction functions?

A. Detect threats and provides a detailed report of discovered threats
B. Proactively detects threats
C. Delivers file with original content
D. Delivers PDF versions of original files with active content removed

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
The SmartEvent R80 Web application for real-time event monitoring is called:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
What SmartEvent component creates events?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
Which Threat Prevention Profile is not included by default in R80 Management?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents/R80/CP_R80BC_ThreatPrevention/136486

QUESTION 200
When using Monitored circuit VRRP, what is a priority delta?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/87911.htm

QUESTION 201
Which of the following is NOT an option to calculate the traffic direction?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 202
When an encrypted packet is decrypted, where does this happen?

A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Which of the following is NOT a component of Check Point Capsule?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/download/products/sg-capsule-solution.pdf

QUESTION 204
You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk54100#1.1.1

QUESTION 205
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 206
Can multiple administrators connect to a Security Management Server at the same time?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265

QUESTION 207
What Identity Agent allows packet tagging and computer authentication?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/62838

QUESTION 208
In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/131914

QUESTION 209
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk105261

QUESTION 210
Which two of these Check Point Protocols are used by _____ ?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 211
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

QUESTION 212
What is the SOLR database for?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Apache_Solr

QUESTION 213
Which of the following commands is used to monitor cluster members?

A. `cphaprob state`
B. `cphaprob status`
C. `cphaprob`
D. `cluster state`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

QUESTION 214
Fill in the blank: Service blades must be attached to a _____.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk80840 **QUESTION 215**
Fill in the blank: An LDAP server holds one or more _____.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/94041

QUESTION 216
Fill in the blank: In Security Gateways R75 and above, SIC uses _____ for encryption.

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/125443

QUESTION 217
What protocol is specifically used for clustered environments?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/5990/FILE/sk31085_Cluster_Control_Protocol_Functionality.pdf

QUESTION 218
Which of the following is NOT a tracking option? (Select three)

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/131914

QUESTION 219
Which command shows the installed licenses?

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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 220
Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 221
Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk106127

QUESTION 222
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 223
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 224
In the Check Point Security Management Architecture, which component(s) can store logs?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 225
Fill in the blank: In order to install a license, it must first be added to the _____.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Non_Gaia_Installation_and_Upgrade_Guide/13128.htm

QUESTION 226
When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/118037

QUESTION 227
Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 228
Which message indicates IKE Phase 2 has completed successfully?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 229
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 230
Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays _____ for the given VPN tunnel.

A. Down

B. No Response
C. Inactive
D. Failed

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_VPN_AdminGuide/14018

QUESTION 231
Which of the following is the most secure means of authentication?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 232
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`

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
QUESTION 233
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SGW_WebAdmin/6721.htm

QUESTION 234
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_ThreatPrevention_WebAdmin/82209.htm

QUESTION 235

Which of the following is an authentication method used for Identity Awareness?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 236
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SIC Status
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.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/125443

QUESTION 237
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/94041

QUESTION 238
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239
Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up
B. There is Load Sharing solution set up
C. Only when there is Unicast solution set up

D. There is High Availability solution set up

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 240
Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

A. Save Policy
B. Install Database
C. Save session
D. Install Policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
From the Gaia web interface, which of the following operations CANNOT be performed on a Security Management Server?

A. Verify a Security Policy
B. Open a terminal shell
C. Add a static route
D. View Security Management GUI Clients

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
Which of the following are types of VPN communities?

A. Pentagon, star, and combination
B. Star, octagon, and combination
C. Combined and star
D. Meshed, star, and combination

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_VPN_AdminGuide/13894

QUESTION 243
What are the three types of UserCheck messages?

A. inform, ask, and block
B. block, action, and warn
C. action, inform, and ask
D. ask, block, and notify

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_DataLossPrevention_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_DataLossPrevention_AdminGuide/94711

QUESTION 244
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 245
Which statement is TRUE of anti-spoofing?

A. Anti-spoofing is not needed when IPS software blade is enabled
B. It is more secure to create anti-spoofing groups manually
C. It is BEST Practice to have anti-spoofing groups in sync with the routing table
D. With dynamic routing enabled, anti-spoofing groups are updated automatically whenever there is a routing change

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

QUESTION 247

How can the changes made by an administrator before publishing the session be seen by a superuser administrator?

A. By impersonating the administrator with the 'Login as…' option
B. They cannot be seen
C. From the SmartView Tracker audit log
D. From **Manage and Settings > Sessions**, right click on the session and click **'View Changes…'**

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248
Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?

A. Application Control
B. Threat Emulation
C. Logging and Status
D. Monitoring

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/downloads/product-related/datasheets/DS_Monitoring.pdf

QUESTION 249
Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

A. 1. Define an accept rule in Security Policy.
   2. Define Security Gateway to hide all internal networks behind the gateway's external IP.
   3. Publish and install the policy.
B. 1. Define an accept rule in Security Policy.
   2. Define automatic NAT for each network to NAT the networks behind a public IP.

3. Publish the policy.

C. 1. Define an accept rule in Security Policy.
2. Define automatic NAT for each network to NAT the networks behind a public IP.
3. Publish and install the policy.

D. 1. Define an accept rule in Security Policy.
2. Define Security Gateway to hide all internal networks behind the gateway's external IP.
3. Publish the policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

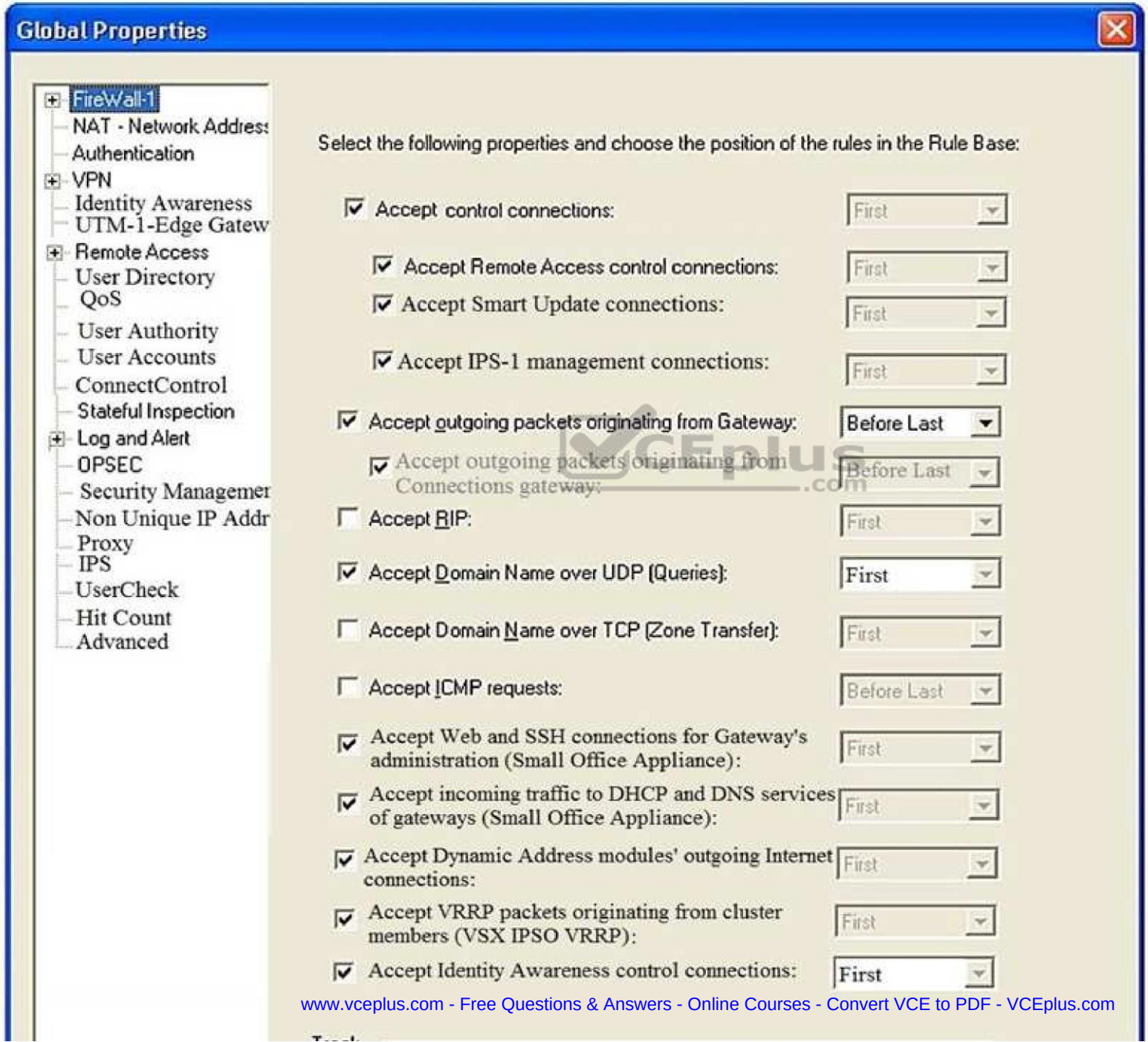
QUESTION 250
True or False: The destination server for Security Gateway logs depends on a Security Management Server configuration.

A. False, log servers are configured on the Log Server General Properties
B. True, all Security Gateways will only forward logs with a SmartCenter Server configuration
C. True, all Security Gateways forward logs automatically to the Security Management Server
D. False, log servers are enabled on the Security Gateway General Properties

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 251
Consider the Global Properties following settings:



The selected option “Accept Domain Name over UDP (Queries)” means:

A. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.
B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
C. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
D. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
How is communication between different Check Point components secured in R80? As with all questions, select the best answer.

A. By using IPSEC
B. By using SIC
C. By using ICA
D. By using 3DES

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/125443

QUESTION 253
Identify the ports to which the Client Authentication daemon listens on by default?

A. 259, 900
B. 256, 257
C. 8080, 529

D. 80, 256

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://digitalcrunch.com/check-point-firewall/list-of-check-point-ports/

QUESTION 254
What is the purpose of the CPCA process?

A. Monitoring the status of processes
B. Sending and receiving logs
C. Communication between GUI clients and the SmartCenter server
D. Generating and modifying certificates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

QUESTION 255
The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run `tcpdump`. How can you achieve this requirement?

A. Add `tcpdump` to CLISH using `add command`.
Create a new access role.
Add `tcpdump` to the role.
Create new user with any UID and assign role to the user.
B. Add `tcpdump` to CLISH using `add command`.
Create a new access role.
Add `tcpdump` to the role.
Create new user with UID 0 and assign role to the user.
C. Create a new access role.

Add expert-mode access to the role.
Create new user with UID 0 and assign role to the user.

D. Create a new access role.
Add expert-mode access to the role.
Create new user with any UID and assign role to the user.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 256
After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24
set static-route default nexthop gateway address 192.168.80.1 on
save config
B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0
add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 on save config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0
add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 on save config
D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24
add static-route default nexthop gateway address 192.168.80.1
on save config

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 257
What Check Point tool is used to automatically update Check Point products for the Gaia OS?

A. Check Point INSPECT Engine

B. Check Point Upgrade Service Engine
C. Check Point Update Engine
D. Check Point Upgrade Installation Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/129978

QUESTION 258
You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

A. Open SmartLog and connect remotely to the IP of the wireless controller
B. Open SmartView Tracker and filter the logs for the IP address of the tablet
C. Open SmartView Tracker and check all the IP logs for the tablet
D. Open SmartLog and query for the IP address of the Manager's tablet

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 259
What are the advantages of a "shared policy" in R80?

A. Allows the administrator to share a policy between all the users identified by the Security Gateway
B. Allows the administrator to share a policy between all the administrators managing the Security Management Server
C. Allows the administrator to share a policy so that it is available to use in another Policy Package
D. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway

Correct Answer: C

Section: (none)
Explanation
Explanation/Reference:

QUESTION 260
To view statistics on detected threats, which Threat Tool would an administrator use?

A. Protections
B. IPS Protections
C. Profiles
D. ThreatWiki

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 261
What is the purpose of a Clean-up Rule?

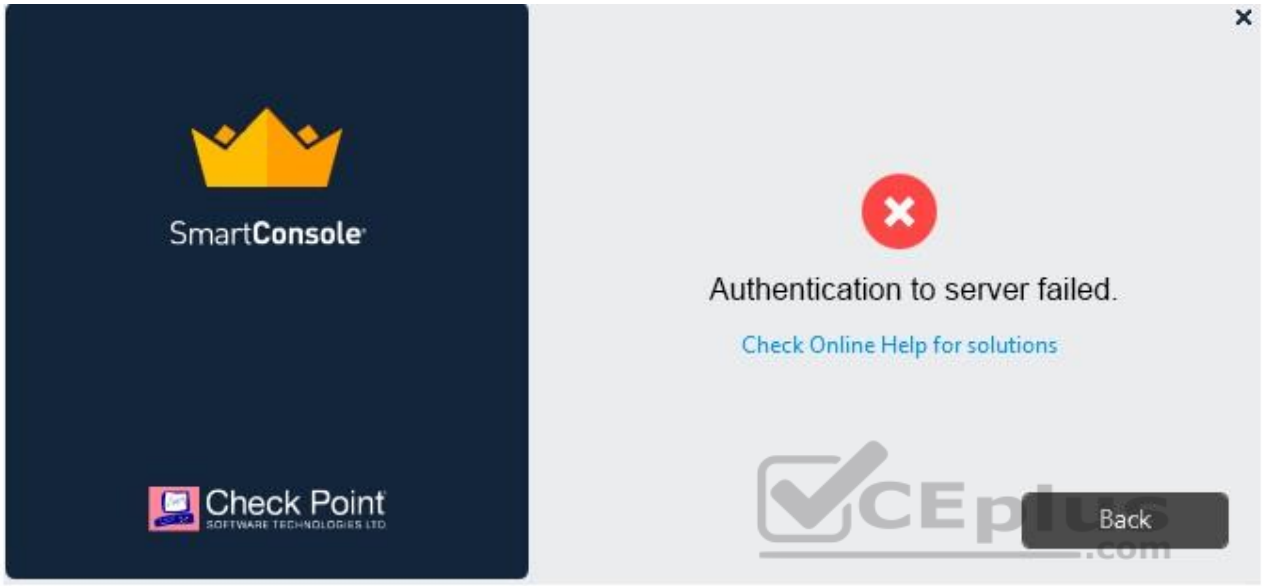
A. Clean-up Rules do not server any purpose.
B. Provide a metric for determining unnecessary rules.
C. To drop any traffic that is not explicitly allowed.
D. Used to better optimize a policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
These are basic access control rules we recommend for all Rule Bases:
- Stealth rule that prevents direct access to the Security Gateway.
- Cleanup rule that drops all traffic that is not allowed by the earlier rules.

There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm **QUESTION 262**
Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.



What is the most likely reason?

A. Check Point R80 SmartConsole authentication is more secure than in previous versions and Vanessa requires a special authentication key for R80 SmartConsole. Check that the correct key details are used.
B. Check Point Management software authentication details are not automatically the same as the Operating System authentication details. Check that she is using the correct details.
C. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.
D. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 263

What is the most complete definition of the difference between the Install Policy button on the SmartConsole's tab, and the Install Policy within a specific policy?

A. The Global one also saves and published the session before installation.
B. The Global one can install multiple selected policies at the same time.
C. The local one does not install the Anti-Malware policy along with the Network policy.
D. The second one pre-select the installation for only the current policy and for the applicable gateways.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
Which of the following is used to initially create trust between a Gateway and Security Management Server?

A. Internal Certificate Authority
B. Token
C. One-time Password
D. Certificate

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/125443

QUESTION 265
Which icon indicates that read/write access is enabled?
A. Pencil
B. Padlock

C. Book
D. Eyeglasses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 266
Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed
B. Kerberos Ticket Requested
C. Account Logon
D. Kerberos Ticket Timed Out

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 267
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or_____.

A. On all satellite gateway to satellite gateway tunnels
B. On specific tunnels for specific gateways
C. On specific tunnels in the community
D. On specific satellite gateway to central gateway tunnels

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:

Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

- Can be specified for an entire community. This option sets every VPN tunnel in the community as permanent.
- Can be specified for a specific Security Gateway. Use this option to configure specific Security Gateways to have permanent tunnels.
- Can be specified for a single VPN tunnel. This feature allows configuring specific tunnels between specific Security Gateways as permanent.

Reference:
https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_VPN_AdminGuide/14018

QUESTION 268
In Unified SmartConsole Gateways and Servers tab you can perform the following functions EXCEPT

A. Upgrade the software version
B. Open WebUI
C. Open SSH
D. Open service request with Check Point Technical Support

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?

A. Log, send snmp trap, email
B. Drop packet, alert, none
C. Log, alert, none
D. Log, allow packets, email

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

Explanation: Configure **Spoof Tracking -** select the tracking action that is done when spoofed packets are detected: ▪ **Log** - Create a log entry (default)
▪ **Alert** - Show an alert
▪ **None** - Do not log or alert

Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 270
Access roles allow the firewall administrator to configure network access according to:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

To create an access role:
1. Select **Users and Administrators** in the Objects Tree.
2. Right-click **Access Roles** > **New Access Role**. The **Access Role** window opens.
3. Enter a **Name** and **Comment** (optional) for the access role.
4. In the **Networks** tab, select one of these: ▪ **Any network**
▪ **Specific networks** - Click the plus sign and select a network.
Your selection is shown in the **Networks** node in the **Role Preview** pane.
5. In the **Users** tab, select one of these: ▪ **Any user**
▪ **All identified users** - Includes users identified by a supported authentication method (internal users, AD users or LDAP users). ▪ **Specific users -** Click the plus sign.
A window opens. You can search for Active Directory entries or select them from the list.

6. In the **Machines** tab, select one of these:

- **Any machine**
- **All identified machines** - Includes machines identified by a supported authentication method (AD). ▪

Specific machines - Click the plus sign.

You can search for AD entries or select them from the list.

7. **Optional:** For computers that use Full Identity Agents, from the **Machines** tab select **Enforce IP spoofing protection**.
8. Click **OK**.

The access role is added to the **Users and Administrators** tree.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92705.htm

QUESTION 271

What are the three deployment considerations for a secure network?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 272

Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

A. All Connections (Clear or Encrypted)
B. Accept all encrypted traffic
C. Specific VPN Communities
D. All Site-to-Site VPN Communities

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
The first rule is the automatic rule for the **Accept All Encrypted Traffic** feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.
2. **Site to site VPN** - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.
3. **Remote access** - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92709.htm

QUESTION 273
One of major features in R80 SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

A. A lock icon shows that a rule or an object is locked and will be available.
B. AdminA and AdminB are editing the same rule at the same time.
C. A lock icon next to a rule informs that any Administrator is working on this particular rule.
D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
In SmartConsole, administrators work with sessions. A session is created each time an administrator logs into SmartConsole. Changes made in the session are saved automatically. These changes are private and available only to the administrator. To avoid configuration conflicts, other administrators see a lock icon on objects and rules that are being edited in other sessions

Reference: http://downloads.checkpoint.com/dc/download.htm?ID=65846

QUESTION 274
When should you generate new licenses?

A. Before installing contract files.
B. After an RMA procedure when the MAC address or serial number of the appliance changes.
C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.

D. Only when the license is upgraded.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk84802

QUESTION 275
Which of the following is NOT a method used by Identity Awareness for acquiring identity?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/products/identity-awareness-software-blade/