

156-215.80.exam.245q

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



Website: <https://vceplus.com>
VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>
Facebook: <https://www.facebook.com/VCE.For.All.VN/>
Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

156-215.80

Check Point Certified Security Administrator R80

Exam A

QUESTION 1

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



<https://vceplus.com/>

- 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 <code>lock database override</code> and <code>unlock database</code> 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	<ul style="list-style-type: none">o <code>lock database override</code>o <code>unlock database</code>

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

QUESTION 2

Examine the following Rule Base.



Standard +

Access Control

- Policy
- NAT

Threat Prevention

- Policy
- Exceptions

Shared Policies

- Geo Policy

Access Tools

- VPN Communities
- Updates
- UserCheck
- Client Certificates
- Application Wks
- Installation History

Install Policy Actions Search for 30 object actions

No.	Name	Source	Destination	VPN	Services & Applications	Action
▼ No Log (1)						
1	Do not log	Any	Any	Any	NBT	Drop
▼ Management Rules (2-3)						
2	Allow Mgmt	Admins	ext-gateway mgmt	Any	https ssh	Accept
3	Stealth Rule	Any	mgmt ext-gateway	Any	Any	Drop
▼ Inbound Rules (4-5)						
4	Web Inbound	Any	webover	Any	http https	Accept
5	Mail Inbound	Any	mailserver	Any	smtp pop-3 imap	Accept
▼ New Section (6)						
6	Webmaster access to servers	Any	webover mailserver	Any	https ssh ftp	Accept
▼ Clean Up (7)						
7	Cleanup rule	Any	Any	Any	Any	Drop

Summary Details Logs History

www.vceplus.com - VCE Exam Simulator - Download A+ VCE (latest) free Open VCE Exams - VCE to PDF Converter - PDF Online

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

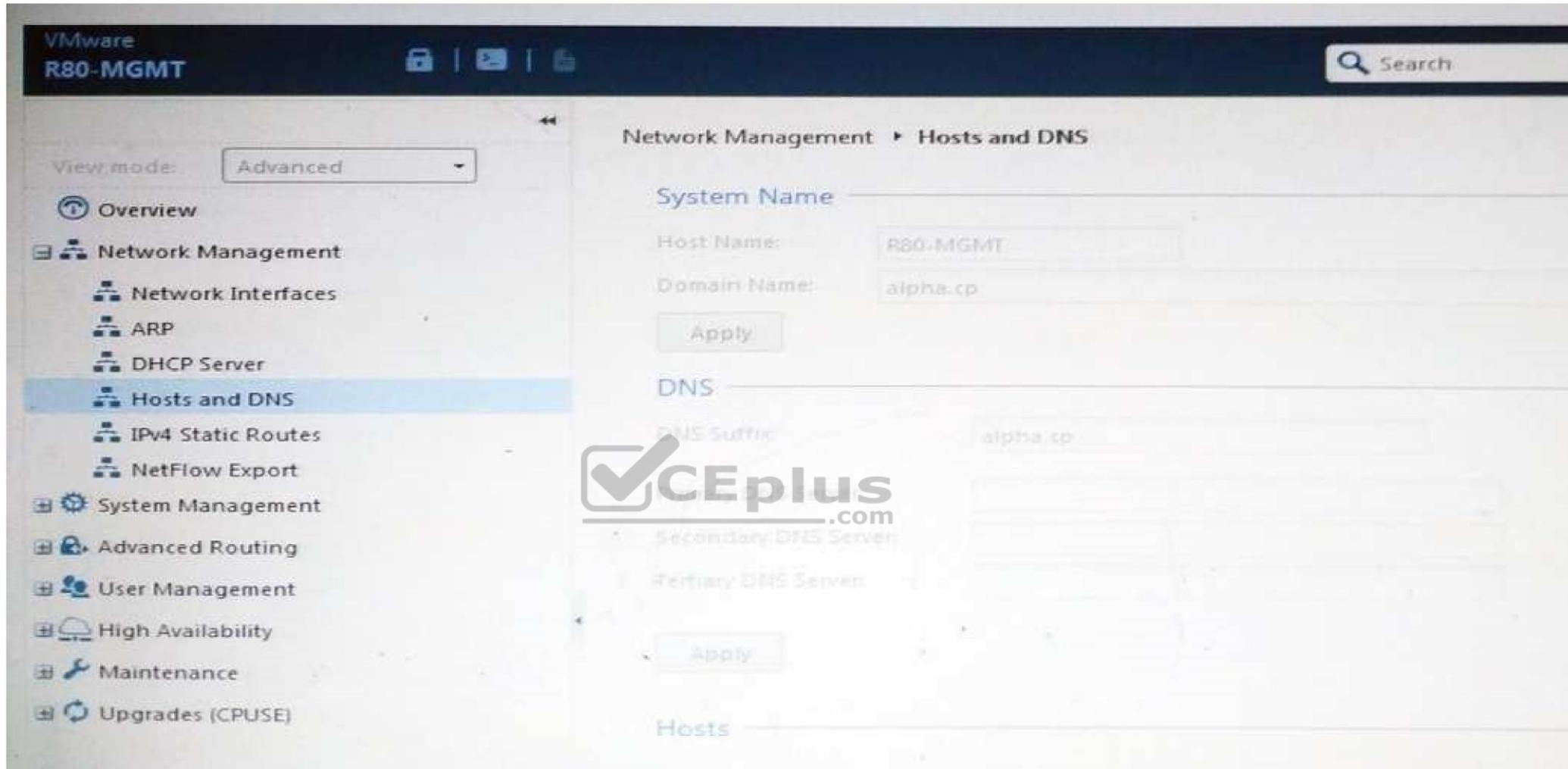
	Description
	Discard changes made during the session.
	Enter session details and see the number of changes made in the session
	Commit policy changes to the database and make them visible to other administrators Note - The changes are saved on the gateways and enforced after the next policy install

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

QUESTION 3

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

- A. The Gaia /bin/confd is locked by another administrator from a SmartConsole session.
- B. The database is locked by another administrator SSH session.



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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

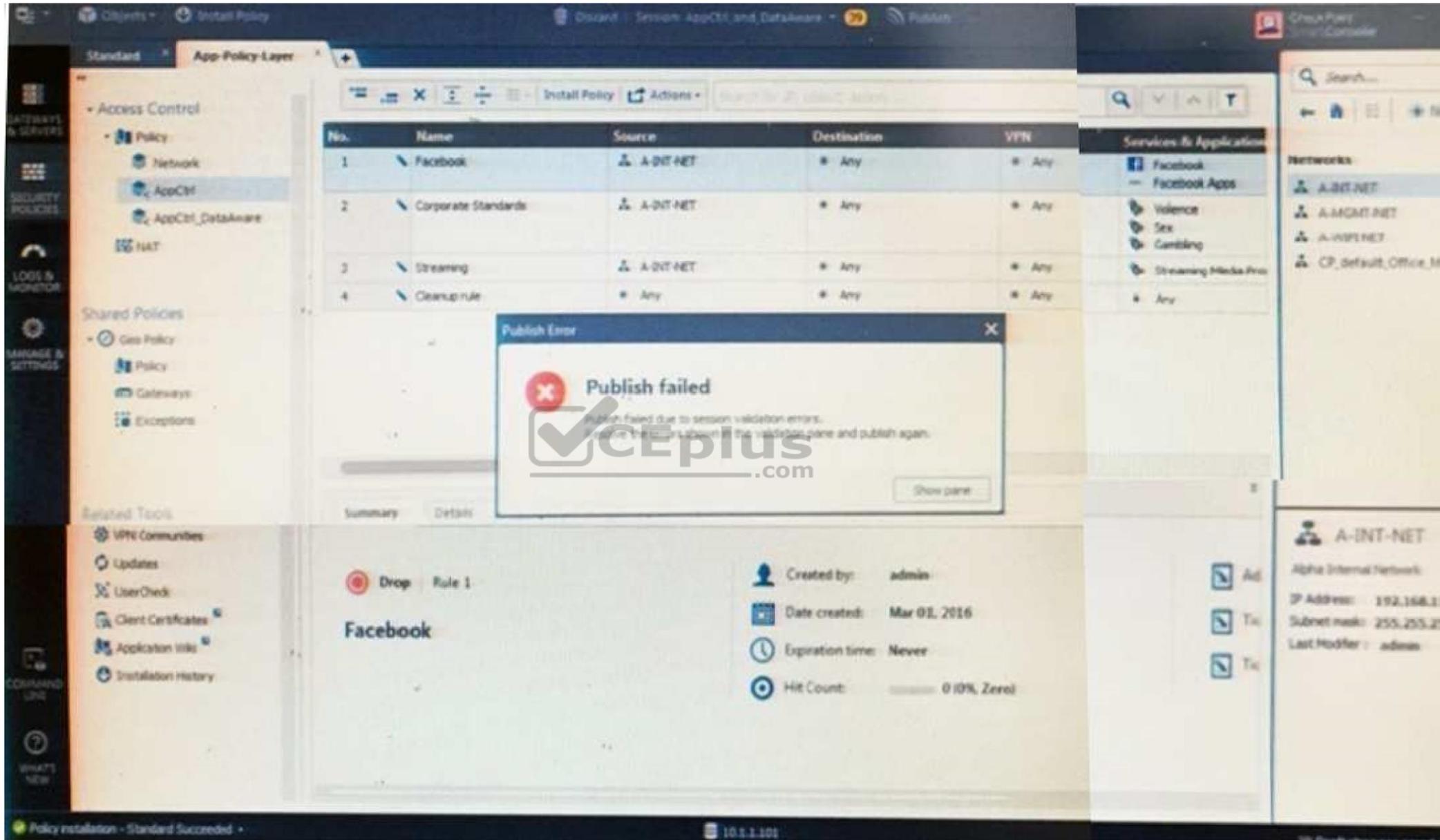
Explanation: There is a lock on top left side of the screen. B is the logical answer.

QUESTION 4

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?





The screenshot displays the Cisco Firepower Management Center (FMC) interface. A central dialog box titled "Publish Error" is open, displaying a red error icon and the text "Publish failed". Below the title, it states: "Publish failed due to session validation errors. Resolve the errors shown in the validation pane and publish again." A "Show pane" button is located at the bottom right of the dialog.

The background interface shows the "App-Policy Layer" configuration page. A table lists the following policies:

No.	Name	Source	Destination	VPN
1	Facebook	A-INT-NET	Any	Any
2	Corporate Standards	A-INT-NET	Any	Any
3	Streaming	A-INT-NET	Any	Any
4	Cleanup rule	Any	Any	Any

Below the table, the "Summary" tab is active, showing details for a "Drop Rule 1" for the "Facebook" application. The details include:

- Created by: admin
- Date created: Mar 01, 2016
- Expiration time: Never
- Hit Count: 0 (0%, Zero)

The left sidebar contains navigation options such as "Access Control", "Shared Policies", and "Related Tools". The right sidebar shows "Services & Application" and "Networks".

- 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 5

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 6

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 7

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 8

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 9

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 10

By default, which port does the WebUI listen on?



<https://vceplus.com/>

A. 80

- B. 4434
- C. 443
- D. 8080

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation: To configure Security Management Server on Gaia:

1. 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 11

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 12

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 13

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: A

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 14

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	<code>/var/log/CPbackup/backups/</code>
	Open Server	<code>/var/CPbackup/backups/</code>
R77.30	Check Point appliances	<code>/var/log/CPbackup/backups/</code>
	Open Server	

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit_doGoviewsolutiondetails=&solutionid=sk91400 **QUESTION 15**

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 16

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 17

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 18

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 19

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 20

When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: SmartUpdate installs two *repositories* on the Security Management server:

- **License & Contract Repository**, which is stored on all platforms in the directory `$FWDIR\conf\`.
- **Package Repository**, which is stored:
 - on Windows machines in `C:\SUroot`.
 - on UNIX machines in `/var/suroot`.

The **Package Repository** requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the **Package Repository**.

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

QUESTION 21

Fill in the blank: The tool _____ generates a R80 Security Gateway configuration report.

- A. `infoCP`
- B. `infoview`



- C. cpinfo
- D. fw cpinfo

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone *cp_uploader* utility for uploading files to Check Point servers).

The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings. When [contacting Check Point Support](#), collect the cpinfo files from the Security Management server and Security Gateways involved in your case.

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92739

QUESTION 22

Which of the following commands can be used to remove site-to-site IPSEC Security Associations (SA)?

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: vpn tu

Description Launch the TunnelUtil tool which is used to control VPN tunnels.

Usage vpn tu
vpn tunnelutil

Example vpn tu

Output

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

(1)          List all IKE SAs

(2)          List all IPsec SAs

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

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

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

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

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

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

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

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

(Q)          Quit
```

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12467.htm#o12627

QUESTION 23

Which of the following is **NOT** an authentication scheme used for accounts created through SmartConsole?



<https://vceplus.com/>

- 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?](http://dl3.checkpoint.com/paid/71/How_to_Configure_Client_Authentication.pdf?HashKey=1479692369_23bc7cdfbeb67c147ec7bb882d557fd4&xtn=.pdf)

[HashKey=1479692369_23bc7cdfbeb67c147ec7bb882d557fd4&xtn=.pdf](http://dl3.checkpoint.com/paid/71/How_to_Configure_Client_Authentication.pdf?HashKey=1479692369_23bc7cdfbeb67c147ec7bb882d557fd4&xtn=.pdf)

QUESTION 24

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 25

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 26

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

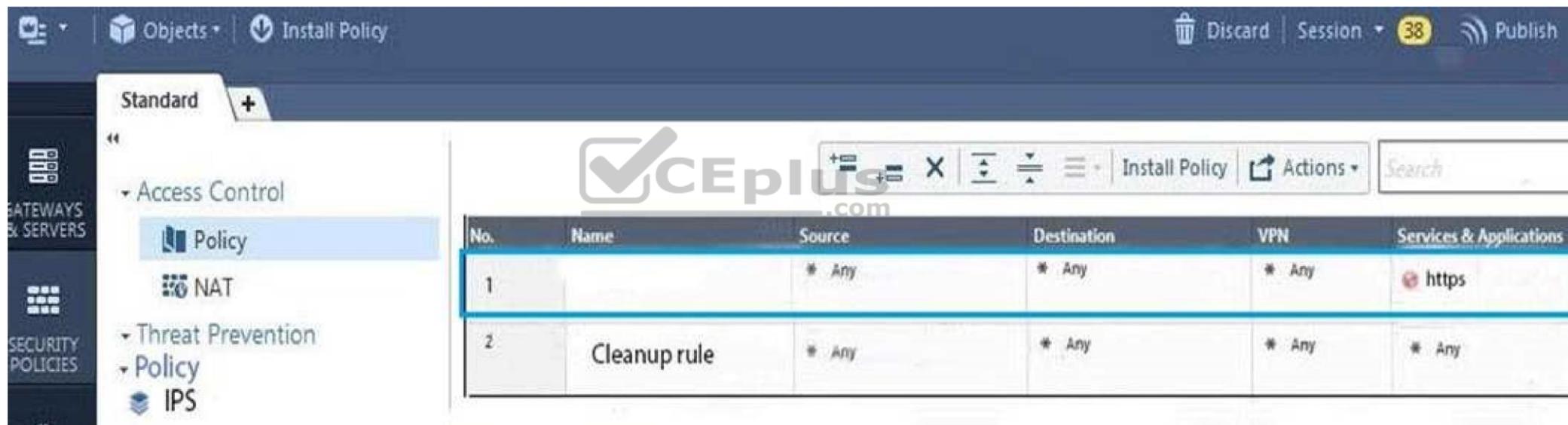
Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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



QUESTION 27

On the following graphic, you will find layers of policies.

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

- 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.

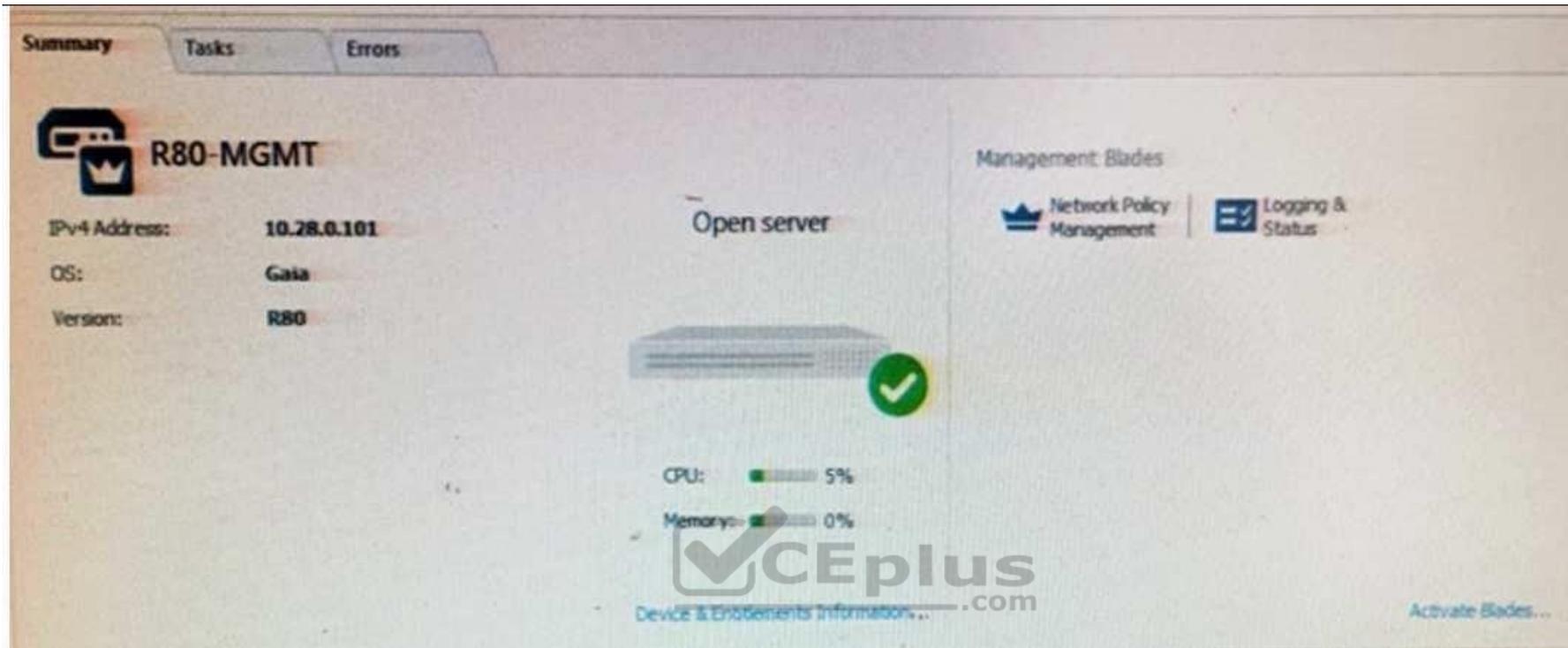
For example, when you upgrade to R80 from earlier versions:

- 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 28

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 29

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 30

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 31

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

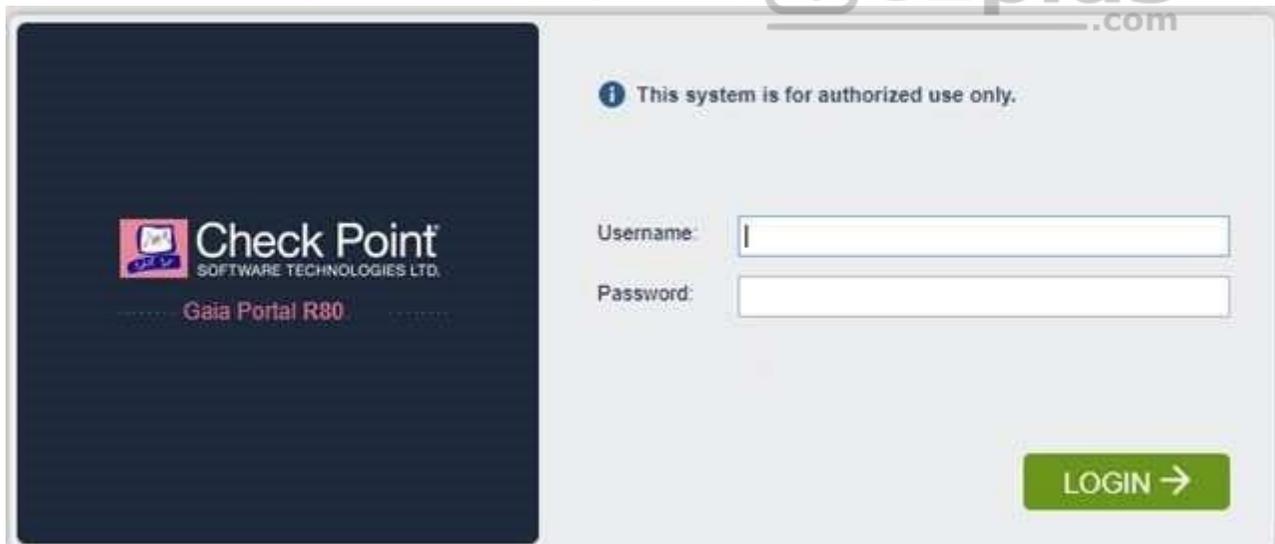
Explanation/Reference:

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 32

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



- A. `set web ssl-port <new port number>`

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

1. 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 'http:ssl_port' /config/db/initial Reference:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482

QUESTION 33

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 34

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 35

Fill in the blank: The _____ collects logs and sends them to the _____ .

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

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 37

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 38

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 39

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 40

The following graphic shows:



<https://vceplus.com/>

Logs - New Tab

Last 7 Days - src:10.1.1.202

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

Time	In	Out	Origin	Source	Source User N...	Destination	Service	Rule	Policy...	Dir...	Source Machine...	Description
Today, 5:30:27 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:30:26 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:56 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:55 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:35 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:34 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:23 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:22 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:00 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:59 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:48 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:47 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:35 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:34 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:23 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:22 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:02 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:01 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:51 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:50 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:23 AM	U	U	A-GW	10.1.1.202		10.1.1.255	no-telegram	1	Standard			
Today, 5:20:18 AM	U	U	A-GW	10.1.1.202		10.1.1.255	no-name	1	Standard			
Today, 5:09:26 AM	U	U	A-GW	10.1.1.202		10.1.1.255	no-telegram	1	Standard			
Today, 5:03:58 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:57 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:52 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:51 AM	U	U	A-GW	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:49 AM	U	U	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 41

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 42

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:

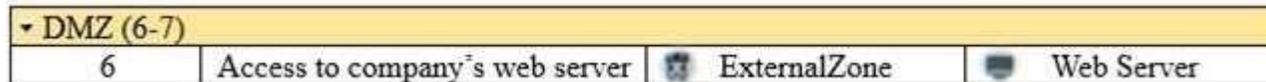
(Should be "migrate import")

"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 43

What does ExternalZone represent in the presented rule?



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

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

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 44

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:

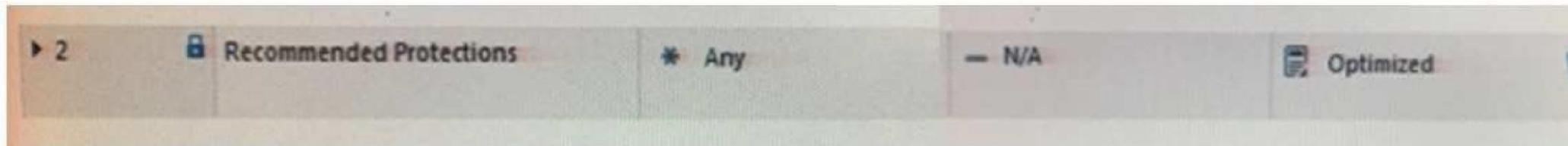
Explanation: Check Point's **FW Monitor** is a powerful built-in tool for capturing network traffic at the packet level. The *FW Monitor* utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark

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

QUESTION 45

View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Administrator Collaboration

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

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

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

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

QUESTION 46

When attempting to start a VPN tunnel, in the logs the error 'no proposal chosen' is seen numerous times. No other VPN-related log entries are present. Which phase of the VPN negotiations has failed?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

Which command is used to add users to or from existing roles?

- A. Add rba user <User Name> roles <List>
- B. Add rba user <User Name>
- C. Add user <User Name> roles <List>

D. Add user <User Name>

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Configuring Roles - CLI (rba)



Description	<ol style="list-style-type: none">1. Add, change or delete role definitions.2. Add or remove users to or from existing roles.3. Add or remove access mechanism (WebUI or CLI) permissions for a specified user.
Syntax	<pre>add rba role <Name> domain-type System readonly-features <List> readwrite-features <List> add rba user <User name> access-mechanisms [Web-UI CLI] add rba user <User Name> roles <List> delete rba role <Name> delete rba role <Name> readonly-features <List> readwrite-features <L delete rba user <User Name> access-mechanisms [Web-UI CLI] delete rba user <User Name> roles <List></pre>

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

QUESTION 48

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

What does this mean?

No.	Name	Source	Destination	VPN	Services & Applications
1	NetBIOS Noise	* Any	* Any	* Any	NET
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh
3	Stealth	* Any	GW-R7730	* Any	* Any
4	DNS	Net_10.28.0.0	* Any	* Any	dns
5	Web	Net_10.28.0.0	* Any	* Any	http https
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp AP-Defender
7	Cleanup rule	* Any	* Any	* Any	* Any

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

Which type of the Check Point license ties the package license to the IP address of the Security Management Server?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50

What is NOT an advantage of Packet Filtering?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation: **Packet Filter Advantages and Disadvantages**



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

Reference: <https://www.checkpoint.com/smb/help/utm1/8.2/7078.htm> **QUESTION 51**

In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

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

Correct Answer: A

Section: (none)

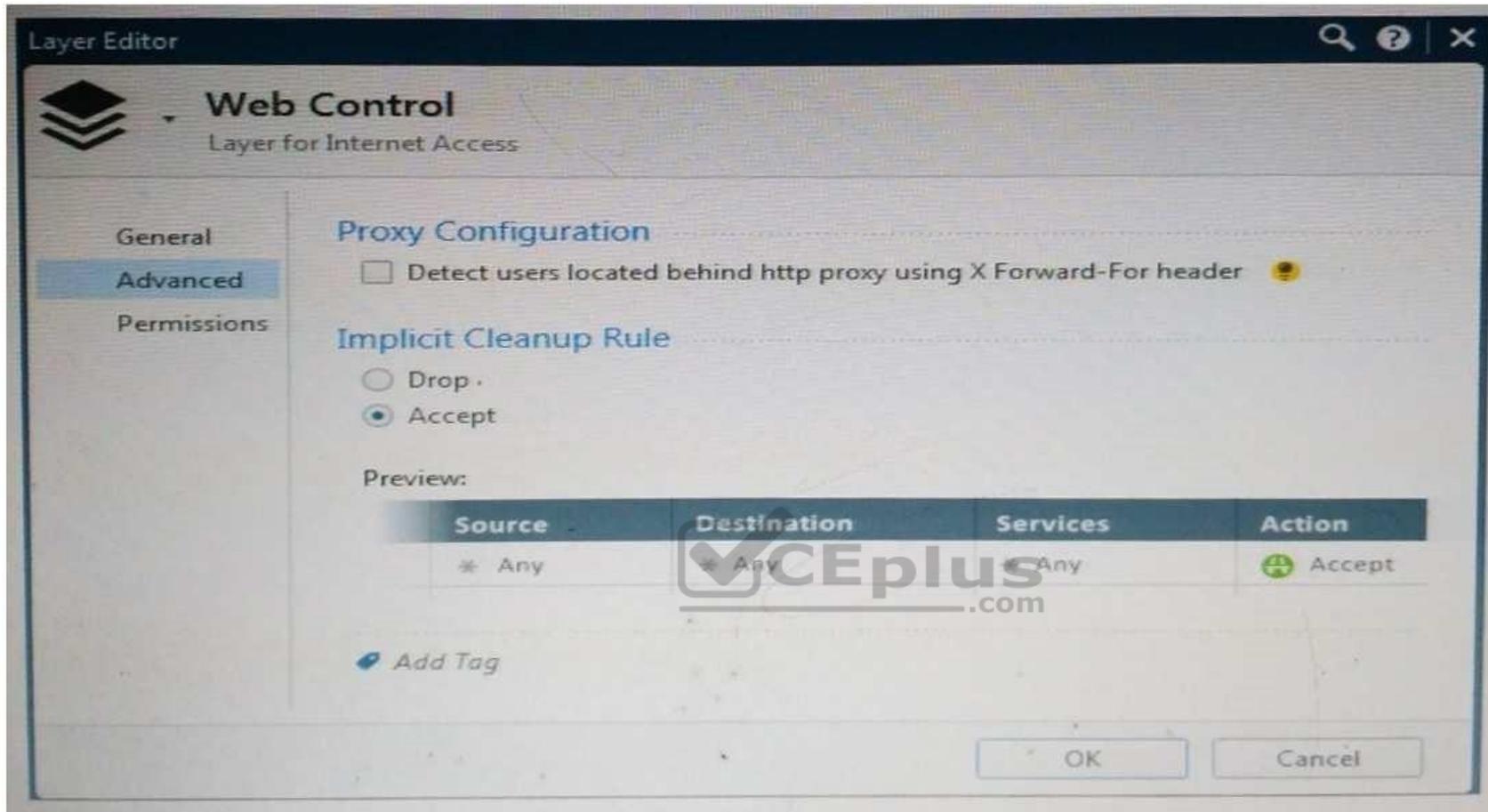
Explanation

Explanation/Reference:

QUESTION 52

Web Control Layer has been set up using the settings in the following dialogue:





Consider the following policy and select the BEST answer.

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

Correct Answer: D

Access To Internet (5)						
5	Access to Internet according to Web control policy	InternalZone	Internet	* Any	* Any	* Any
5.1	DNS server should have access to	DNS	ExternalZone	* Any	dns	* Any
5.2	Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	* Any	Inappropriate Sites	* Any
5.3	HR can access to social network applications	HR	Internet	* Any	Facebook Twitter LinkedIn	* Any
5.4	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	* Any	YouTube Vimeo	* Any
5.5	Block specific URLs	* Any	Internet	* Any	Blocked URLs	* Any
5.6	Block specific categories for all employees	Corporate LANs Branch Office LAN	Internet	* Any	Social Networking Streaming Media Pr... P2P File Sharing	* Any

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Policy Layers and Sub-Policies

R80 introduces the concept of layers and sub-policies, allowing you to segment your policy according to your network segments or business units/functions. In addition, you can also assign granular privileges by layer or sub-policy to distribute workload and tasks to the most qualified administrators

- With layers, the rule base is organized into a set of security rules. These set of rules or layers, are inspected in the order in which they are defined, allowing control over the rule base flow and the security functionalities that take precedence. If an “accept” action is performed across a layer, the inspection will continue to the next layer. For example, a compliance layer can be created to overlay across a cross-section of rules.
- Sub-policies are sets of rules that are created for a specific network segment, branch office or business unit, so if a rule is matched, inspection will continue through this subset of rules before it moves on to the next rule.
- Sub-policies and layers can be managed by specific administrators, according to their permissions profiles. This facilitates task delegation and workload distribution.

Reference: <https://community.checkpoint.com/docs/DOC-1065>

QUESTION 53

Which of the following are types of VPN communicates?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

Fill in the blank: RADIUS protocol uses _____ to communicate with the gateway.

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: **Parameters:**

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

Reference: https://sc1.checkpoint.com/documents/R76SP/CP_R76SP_Security_System_WebAdminGuide/105209.htm

QUESTION 55

When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

- A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
- B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
- C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
- D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

Office mode means that:

- A. SecureID client assigns a routable MAC address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
- B. Users authenticate with an Internet browser and use secure HTTPS connection.
- C. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
- D. Allows a security gateway to assign a remote client an IP address. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Office Mode enables a Security Gateway to assign internal IP addresses to SecureClient users. This IP address will not be exposed to the public network, but is encapsulated inside the VPN tunnel between the client and the Gateway. The IP to be used externally should be assigned to the client in the usual way by the Internet Service provider used for the Internet connection. This mode allows a Security Administrator to control which addresses are used by remote clients inside the local network and makes them part of the local network. The mechanism is based on an IKE protocol extension through which the Security Gateway can send an internal IP address to the client.

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30545

QUESTION 57

Administrator wishes to update IPS from SmartConsole by clicking on the option “**update now**” under the IPS tab. Which device requires internet access for the update to work?

- A. Security Gateway
- B. Device where SmartConsole is installed
- C. SMS
- D. SmartEvent

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Updating IPS Manually

You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website. You can only manually update IPS if a proxy is defined in Internet Explorer settings.

To obtain updates of all the latest protections from the IPS website:

1. Configure the settings for the proxy server in Internet Explorer.
 1. In Microsoft Internet Explorer, open **Tools > Internet Options > Connections tab > LAN Settings**.
The LAN Settings window opens.
 2. Select **Use a proxy server for your LAN**.
 3. Configure the IP address and port number for the proxy server.
 4. Click **OK**.

The settings for the Internet Explorer proxy server are configured.

2. In the IPS tab, select **Download Updates** and click **Update Now**.

If you chose to automatically mark new protections for Follow Up, you have the option to open the Follow Up page directly to see the new protections.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IPS_AdminGuide/12850.htm

QUESTION 58

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: Did you know: mgmt_cli can accept csv files as inputs using the --batch option.

The first row should contain the argument names and the rows below it should hold the values for these parameters.

So an equivalent solution to the powershell script could look like this:

data.csv:

name	ip v4-address	color
host1	192.168.35.1	black
host2	192.168.35.2	red
host3	192.168.35.3	blue

mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server>

This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

Reference: <https://community.checkpoint.com/thread/1342> <https://sc1.checkpoint.com/documents/R80/APIs/#gui-cli/add-access-rule>

QUESTION 59

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?



<https://vceplus.com/>

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Identity Awareness gets identities from these acquisition sources:

- AD Query
- Browser-Based Authentication
- Endpoint Identity Agent
- Terminal Servers Identity Agent
- Remote Access Reference:

https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62007.htm

QUESTION 60

Which of the following is NOT a back up method?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: The built-in Gaia backup procedures:

- Snapshot Management
- System Backup (and System Restore)
- Save/Show Configuration (and Load Configuration)

Check Point provides three different procedures for backing up (and restoring) the operating system and networking parameters on your appliances. ▪ Snapshot (Revert) ▪ Backup (Restore) ▪ upgrade_export (Migrate)

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk54100

QUESTION 61

Which of the following is NOT an advantage to using multiple LDAP servers?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 62

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

<https://www.checkpoint.com/products/antivirus-software-blade/>

QUESTION 63

What is the default method for destination NAT?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: **Client Side NAT** - destination is NAT'd by the inbound kernel

QUESTION 64

Choose what BEST describes a Session.

- A. Starts when an Administrator publishes all the changes made on SmartConsole.
- B. Starts when an Administrator logs in to the Security Management Server through SmartConsole and ends when it is published.
- C. Sessions ends when policy is pushed to the Security Gateway.
- D. Sessions locks the policy package for editing.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Administrator Collaboration

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

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

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

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

QUESTION 65

Which of the following is **NOT** a VPN routing option available in a star community?

- A. To satellites through center only

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

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

SmartConsole

For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:

1. On the **Star Community** window, in the:
 - a. **Center Gateways** section, select the Security Gateway that functions as the "Hub".
 - b. **Satellite Gateways** section, select Security Gateways as the "spokes", or satellites.
2. On the **VPN Routing** page, **Enable VPN routing for satellites** section, select one of these options:
 - a. **To center and to other Satellites through center** - This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security Gateway with a static IP address.
 - b. **To center, or through the center to other satellites, to internet and other VPN targets** - This allows connectivity between the Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.
3. Create an appropriate Access Control Policy rule.
4. NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.

The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80BC_VPN/html_frameset.htm

QUESTION 66

What is the default shell of Gaia CLI?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: This chapter gives an introduction to the Gaia command line interface (CLI).

The default shell of the CLI is called `clish`.

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

QUESTION 67

Which of the following licenses are considered temporary?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 68

Where can administrator edit a list of trusted SmartConsole clients in R80?

- A. `cpconfig` on a Security Management Server, in the WebUI logged into a Security Management Server.
- B. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
- C. In `cpconfig` on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: **Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients**.
- D. WebUI client logged to Security Management Server, SmartDashboard: **Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients**, via `cpconfig` on a Security Gateway.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is _____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment. Which details she need to fill in System Restore window before she can click OK button and test the backup?

- A. Server, SCP, Username, Password, Path, Comment, Member
- B. Server, TFTP, Username, Password, Path, Comment, All Members
- C. Server, Protocol, Username, Password, Path, Comment, All Members
- D. Server, Protocol, Username, Password, Path, Comment, member

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

On the following picture an administrator configures Identity Awareness:

Check Point Gateway - A-GW

General Properties

- Network Management
- NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Anti-Bot and Anti-Virus
- Platform Portal
- UserCheck
- Mail
- IPS
- VP
- Mo
- Dat
- Mo
- Log
- Fet
- Opt
- Uth

Machine

Name: Color:

IPv4 Address: Dynamic Address

IPv6 Address:

Identity Awareness Configuration

Methods For Acquiring Identity

Select how users will be identified by your security gateway.

- AD Query**
The gateway seamlessly identifies Active Directory users and computers.
- Browser-Based Authentication**
Transparent Kerberos authentication or Captive Portal.
- Terminal Servers**
Identify individual users traffic coming from terminal servers (e.g. Citrix).
An agent is required on the terminal server.

ies:

After clicking "Next" the above configuration is supported by:

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

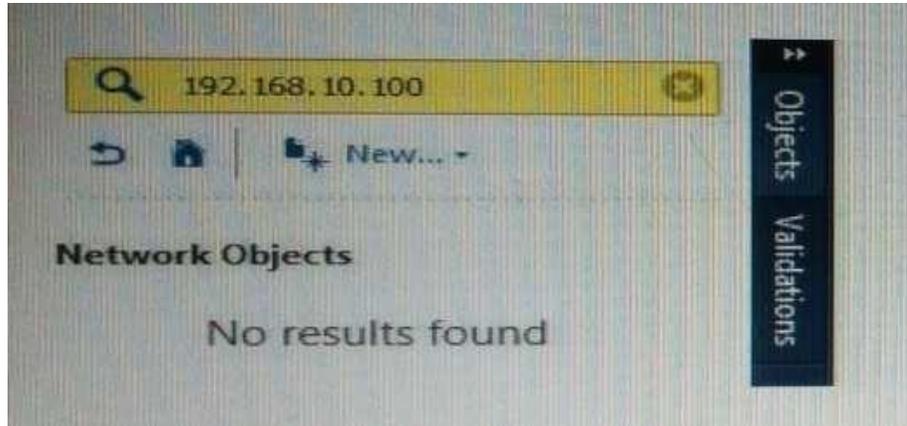
Explanation: To enable Identity Awareness:

1. Log in to R80 SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Gateway on which to enable Identity Awareness.
3. On the Network Security tab, select **Identity Awareness**. The **Identity Awareness** Configuration wizard opens.
4. 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).

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80BC_IdentityAwareness/html_frameset.htm?topic=documents/R80/CP_R80BC_IdentityAwareness/62050

QUESTION 72

What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.



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

Correct Answer: B

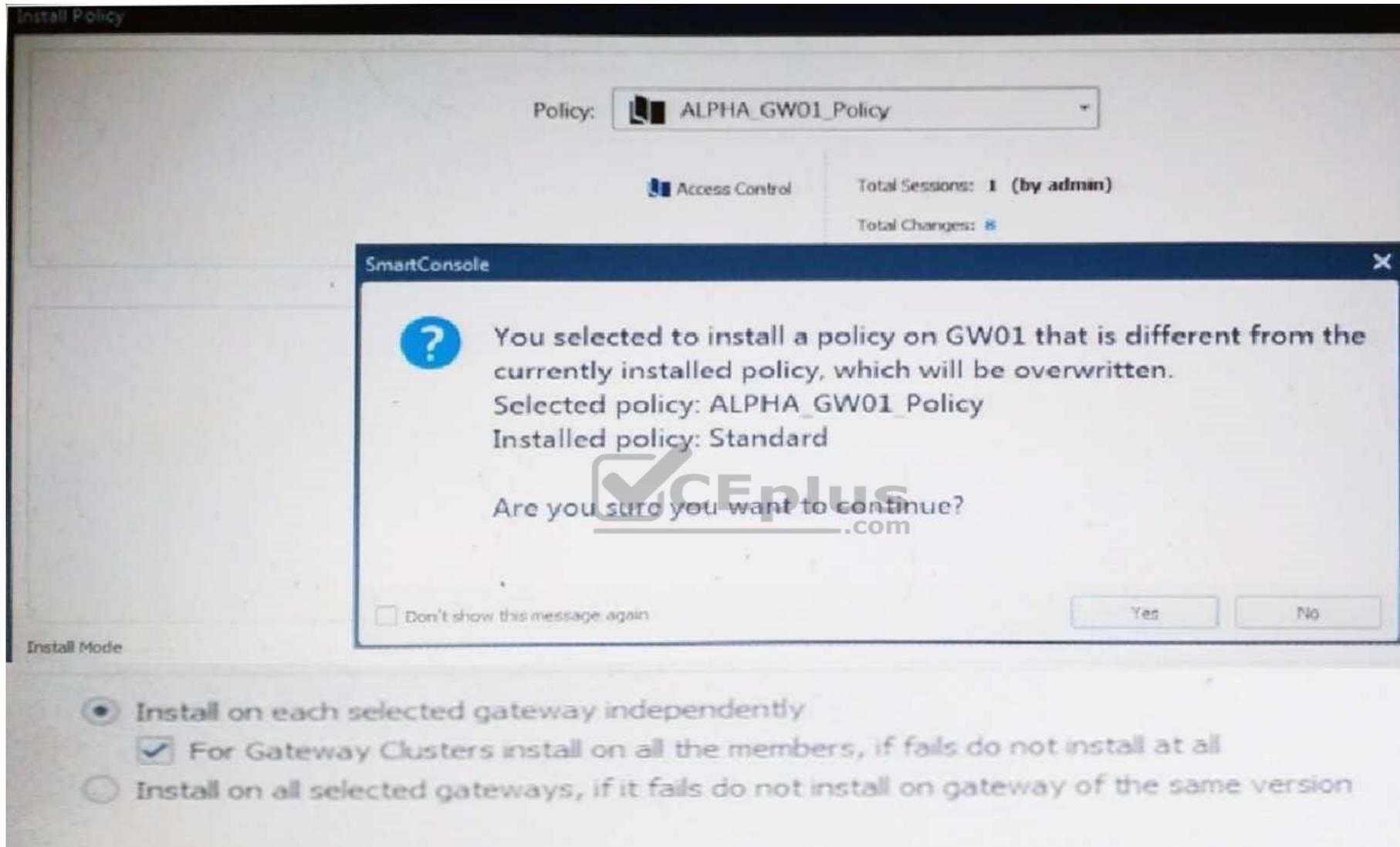
Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

Why would an administrator see the message below?



- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.

D. A new Policy Package created on the Gateway and transferred to the management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 74

Fill in the blank: The _____ software blade enables Application Security policies to allow, block, or limit website access based on user, group, and machine identities.

- A. Application Control
- B. Data Awareness
- C. URL Filtering
- D. Threat Emulation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 75

At what point is the Internal Certificate Authority (ICA) created?

- A. Upon creation of a certificate
- B. During the primary Security Management Server installation process.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: Introduction to the ICA

The ICA is a Certificate Authority which is an integral part of the Check Point product suite. It is fully compliant with X.509 standards for both certificates and CRLs. See the relevant X.509 and PKI documentation, as well as RFC 2459 standards for more information. You can read more about Check Point and PKI in the [R76 VPN Administration Guide](#).

The ICA is located on the Security Management server. It is created during the installation process, when the Security Management server is configured.

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/13118

QUESTION 76

In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?



<https://vceplus.com/>



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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

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

QUESTION 77

Which information is included in the “Full Log” tracking option, but is not included in the “Log” tracking option?

- A. file attributes

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: Tracking Options

- **Network Log** - Generates a log with only basic Firewall information: Source, Destination, Source Port, Destination Port, and Protocol.
- **Log** - Equivalent to the Network Log option, but also includes the application name (for example, Dropbox), and application information (for example, the URL of the Website). This is the default Tracking option.
- **Full Log** - Equivalent to the log option, but also records data for each URL request made.
 - If suppression is not selected, it generates a **complete log** (as defined in pre-R80 management).
 - If suppression is selected, it generates an **extended log** (as defined in pre-R80 management).

None - Do not generate a log.

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

QUESTION 78

In the R80 SmartConsole, on which tab are Permissions and Administrators defined?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

- A. Full
- B. Light

- C. Custom
- D. Complete

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 80

Fill in the blanks: The Application Layer Firewalls inspect traffic through the _____ layer(s) of the TCP/IP model and up to and including the _____ layer.

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 81

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: What Happens When a Security Gateway Recovers?

In a Load Sharing configuration, when the failed Security Gateway in a cluster recovers, all connections are redistributed among all active members. High Availability and Load Sharing in ClusterXL ClusterXL Administration Guide R77 Versions | 31 In a High Availability configuration, when the failed Security Gateway in a cluster recovers, the recovery method depends on the configured cluster setting. The options are:

- Maintain Current Active Security Gateway means that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events.
- Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

Reference: http://dl3.checkpoint.com/paid/7e/7ef174cf00762ceaf228384ea20ea64a/CP_R77_ClusterXL_AdminGuide.pdf?HashKey=1479822138_31410b1f8360074be87fd8f1ab682464&xtn=.pdf

QUESTION 82

After the initial installation the First Time Configuration Wizard should be run. Select the BEST answer.

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Check Point Security Gateway and Check Point Security Management require running the First Time Configuration Wizard in order to be configured correctly. The First Time Configuration Wizard is available in Gaia Portal and also through CLI.

To invoke the First Time Configuration Wizard through CLI, run the **config_system** command from the Expert shell.

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk111119

QUESTION 83

In order to modify Security Policies the administrator can use which of the following tools? Select the BEST answer.

- A. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
- B. SmartConsole and WebUI on the Security Management Server.

- C. mgmt_cli or WebUI on Security Gateway and SmartConsole on the Security Management Server.
- D. SmartConsole or mgmt_cli on any computer where SmartConsole is installed.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 84

Which of the following is NOT an element of VPN Simplified Mode and VPN Communities?

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

Explanation: Migrating from Traditional Mode to Simplified Mode

To migrate from Traditional Mode VPN to Simplified Mode:

1. On the **Global Properties** > **VPN** page, select one of these options:

• **Simplified mode to all new Firewall Policies** •

Traditional or Simplified per new Firewall Policy

2. Click **OK**.

3. From the R80 SmartConsole **Menu**, select **Manage policies**.

The **Manage Policies** window opens.

4. Click **New**.

The **New Policy** window opens.

5. Give a name to the new policy and select **Access Control**.

In the Security Policy Rule Base, a new column marked **VPN** shows and the **Encrypt** option is no longer available in the **Action** column. You are now working in Simplified Mode.

Reference: http://dl3.checkpoint.com/paid/05/05e695b2012b4fd1d2bdfeccecd29290/CP_R80BC_VPN_AdminGuide.pdf?

[HashKey=1479823792_55fbc10656c87db4fcf742f4899ba90d&xtn=.pdf](#)

QUESTION 85

Fill in the blanks: A Check Point software license consists of a _____ and _____ .

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

Software Blades

- Container

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk11054

QUESTION 86

Fill in the blank: Once a license is activated, a _____ should be installed.

- A. License Management file
- B. Security Gateway Contract file
- C. Service Contract file
- D. License Contract file

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Service Contract File

Following the activation of the license, a Service Contract File should be installed. This file contains important information about all subscriptions purchased for a specific device and is installed via SmartUpdate. A detailed explanation of the Service Contract File can be found in [sk33089](#). Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk11054 **QUESTION 87**

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 88

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 89

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 90

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: D

Section: (none)

Explanation

Explanation/Reference:

Explanation: **SandBlast Threat Emulation**

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

Reference: <https://www.checkpoint.com/products/next-generation-threat-prevention/>

QUESTION 91

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 92

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 93

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 94

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 95

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 96

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 97

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 98

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 99



<https://vceplus.com/>

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 100

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: 3. System Backup (and System Restore)

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

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

QUESTION 101

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 102

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: 2. Snapshot Management**

The snapshot creates a binary image of the entire root (*/v_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 103

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

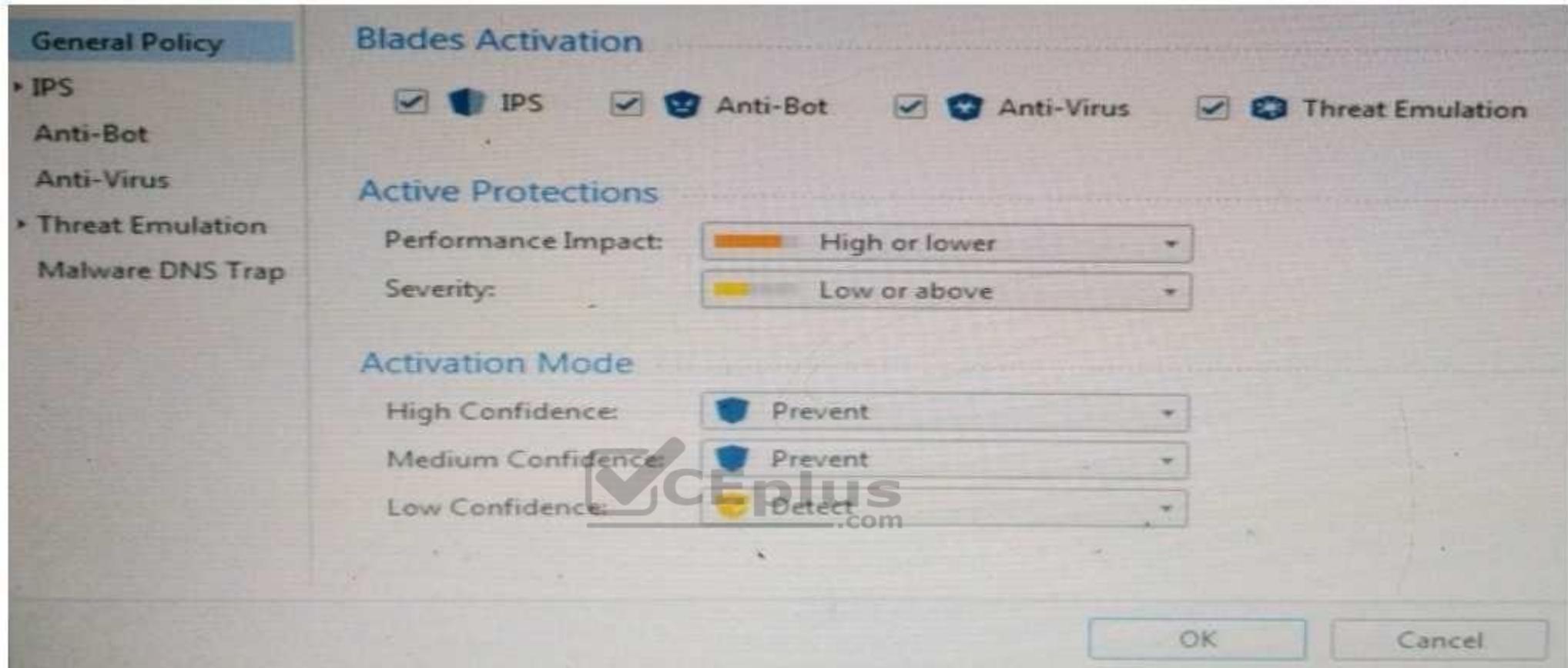
R80 Management Servers can manage gateways of these versions:

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 104

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 105

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 106

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

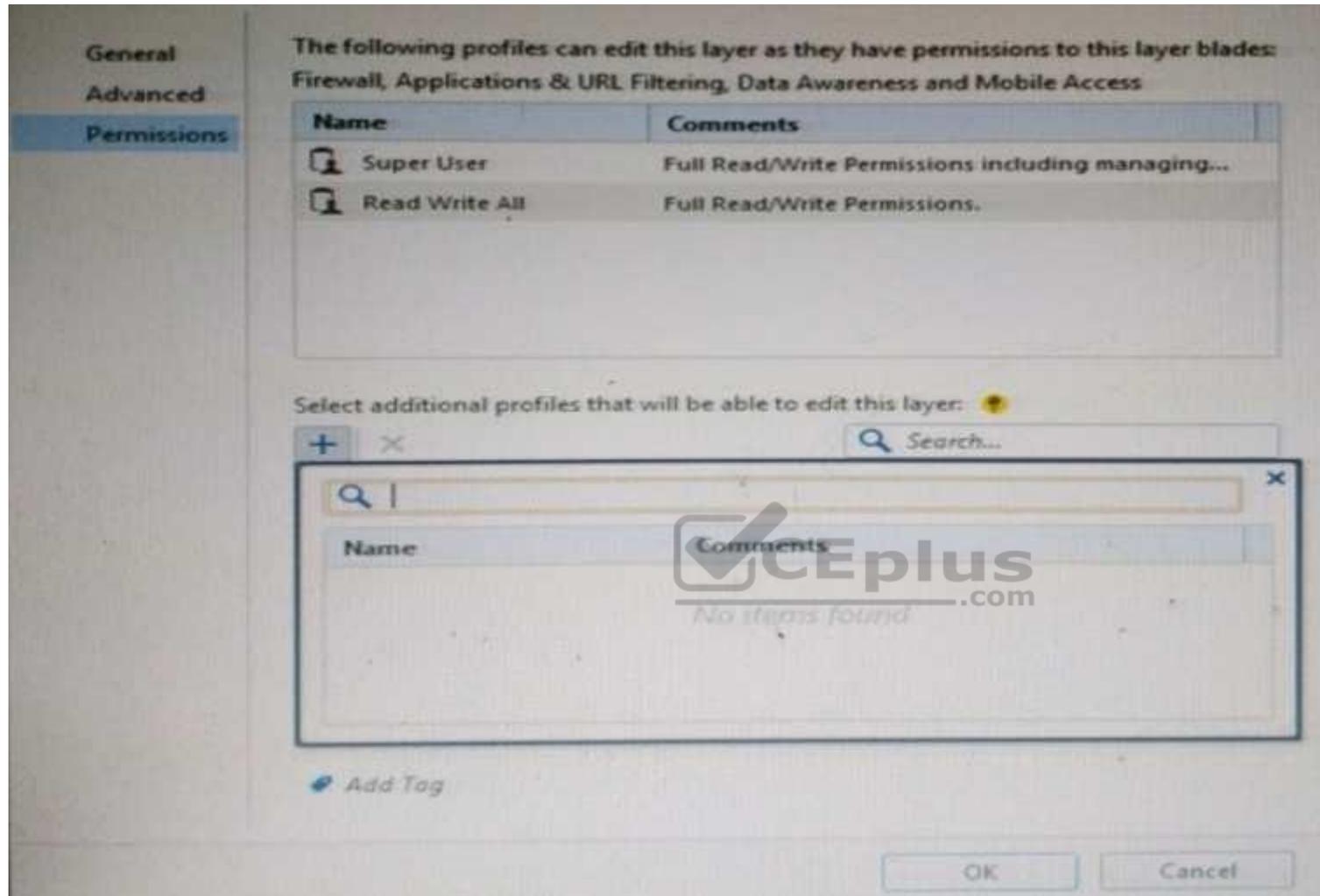
Section: (none)

Explanation

Explanation/Reference:

QUESTION 107

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.
- 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 108

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 109

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 110

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 111

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 112

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 John'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 113

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 114

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 115

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 116

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 117

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 118

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 119

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 120

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:



QUESTION 121

Choose the SmartLog property that is TRUE.



<https://vceplus.com/>

- A. SmartLog has been an option since release R71.10.
- B. SmartLog is not a Check Point product.

- C. SmartLog and SmartView Tracker are mutually exclusive.
- D. SmartLog is a client of SmartConsole that enables enterprises to centrally track log records and security activity with Google-like search.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 122

Which directory holds the SmartLog index files by default?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 123

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 124

Can a Check Point gateway translate both source IP address and destination IP address in a given packet?

- A. Yes.
- B. No.
- C. Yes, but only when using Automatic NAT.
- D. Yes, but only when using Manual NAT.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 125

Which of the following is NOT defined by an Access Role object?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 126

You installed Security Management Server on a computer using GAiA in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second GAiA computer, which you plan to ship to another Administrator at a MegaCorp hub office. What is the correct order for pushing SIC certificates to the Gateway before shipping it?

1. Run cpconfig on the Gateway, select **Secure Internal Communication**, enter the activation key, and reconfirm.
2. Initialize Internal Certificate Authority (ICA) on the Security Management Server.
3. Configure the Gateway object with the host name and IP addresses for the remote site.

4. Click the **Communication** button in the Gateway object's **General** screen, enter the activation key, and click **Initialize** and **OK**.
5. Install the Security Policy.

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

Correct Answer: B

Section: (none)

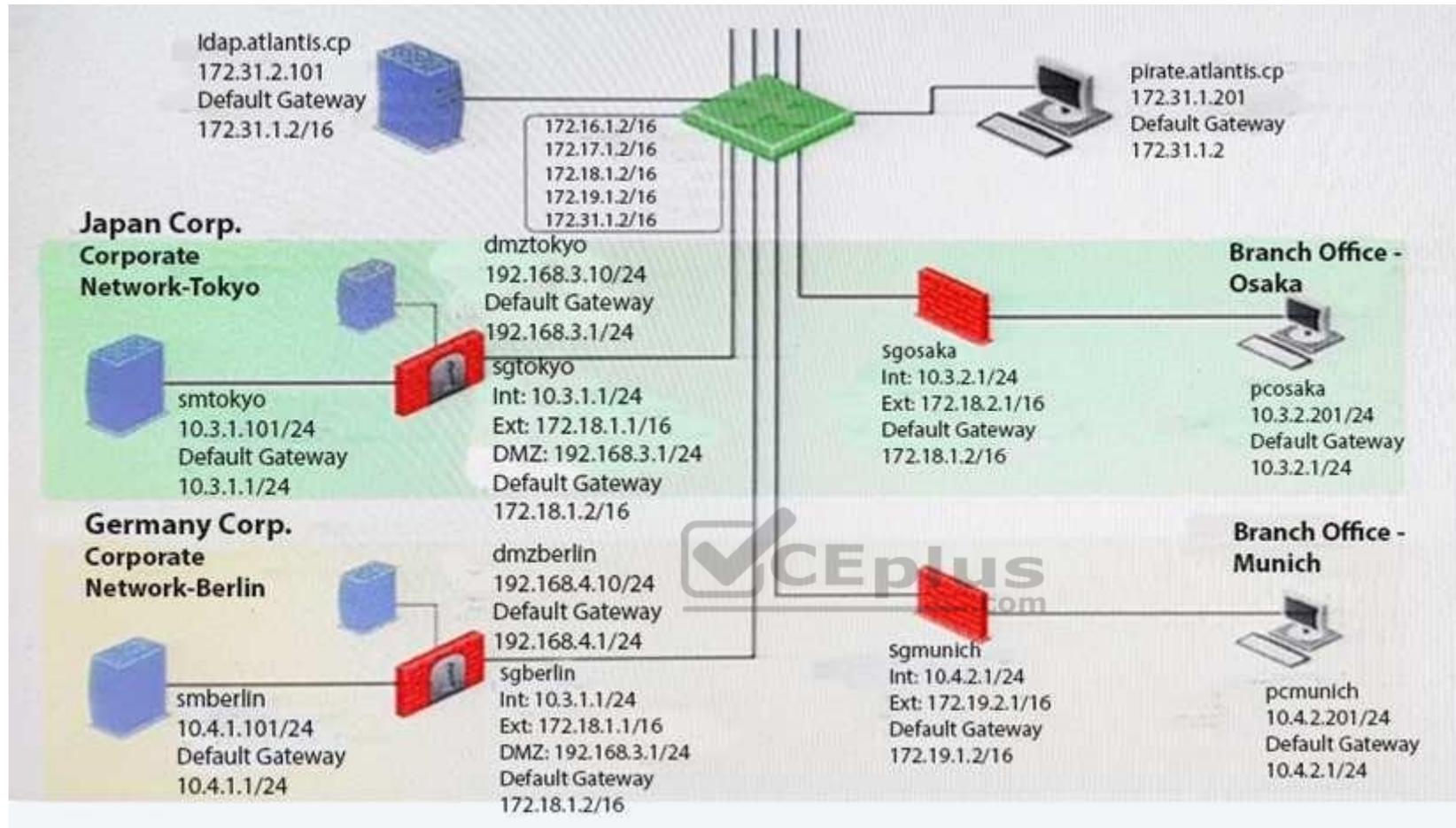
Explanation

Explanation/Reference:

QUESTION 127

You want to reset SIC between **smberlin** and **sgosaka**.





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



What is the reason for this behavior?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 128

Which of these components does NOT require a Security Gateway R77 license?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 129

What statement is true regarding Visitor Mode?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 130

Mesh and Star are two types of VPN topologies. Which statement below is TRUE about these types of communities?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 131

What CLI utility allows an administrator to capture traffic along the firewall inspection chain?

- A. `show interface (interface) -chain`

- B. tcpdump
- C. tcpdump /snoop
- D. fw monitor

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 132

Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 133

NAT can NOT be configured on which of the following objects?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 134

The `fw monitor` utility is used to troubleshoot which of the following problems?

- A. Phase two key negotiation
- B. Address translation
- C. Log Consolidation Engine
- D. User data base corruption

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how many often the particular rules match. Where can you see it? Give the BEST answer.

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

Correct Answer: C

Section: (none)

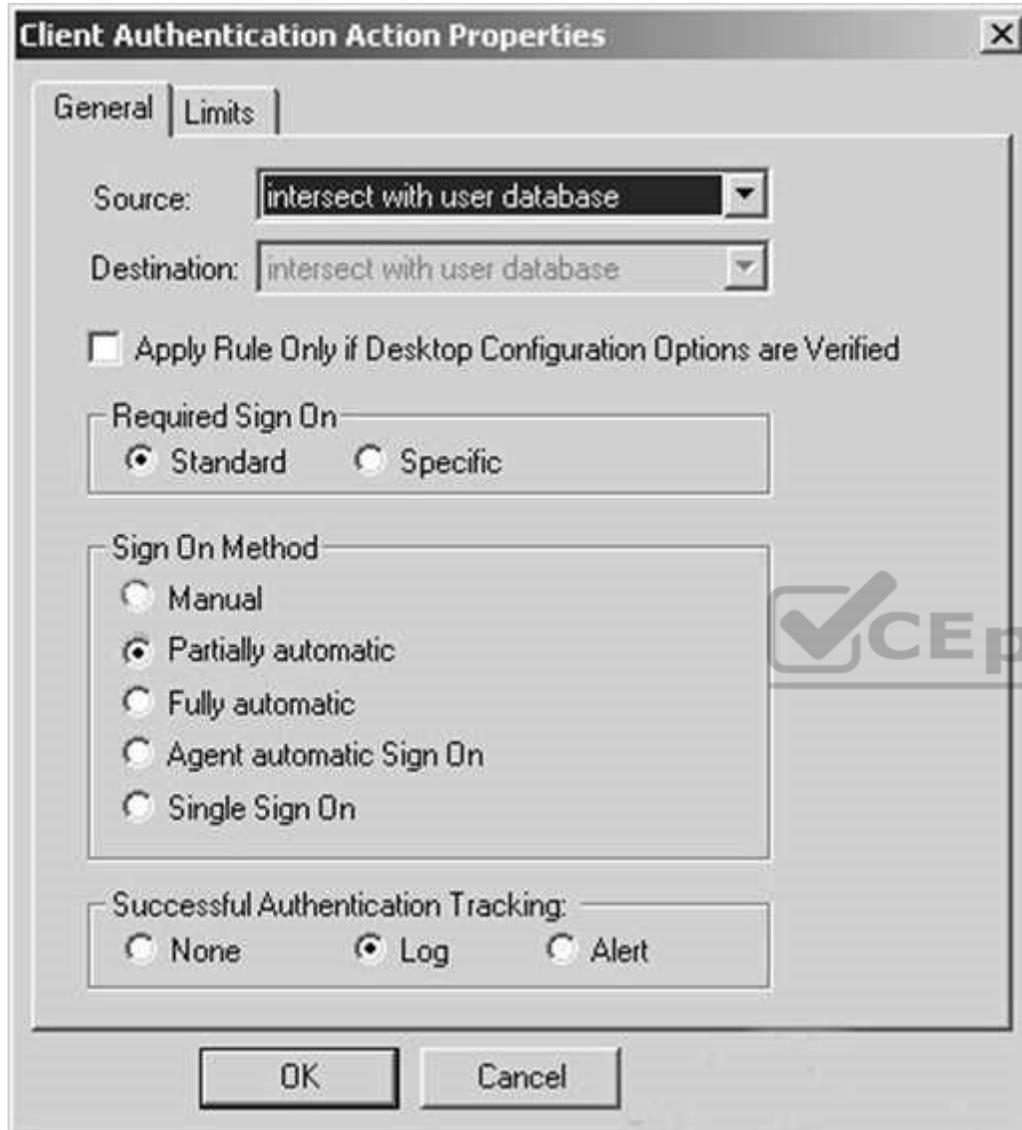
Explanation

Explanation/Reference:

QUESTION 136

Study the Rule base and **Client Authentication Action** properties screen.

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



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

A. user is prompted for authentication by the Security Gateways again.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137

What are the three tabs available in SmartView Tracker?

- A. Network & Endpoint, Management, and Active
- B. Network, Endpoint, and Active
- C. Predefined, All Records, Custom Queries
- D. Endpoint, Active, and Custom Queries

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:



QUESTION 138

In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

- A. Rule 0
- B. Blank field under Rule Number
- C. Rule 1
- D. Cleanup Rule

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

QUESTION 139

Which SmartConsole component can Administrators use to track changes to the Rule Base?

- A. WebUI
- B. SmartView Tracker
- C. SmartView Monitor
- D. SmartReporter

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 140

Which set of objects have an **Authentication** tab?

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 141

Which rule is responsible for the user authentication failure?

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None
2	0	Management	webSingapore	fwsingapore	Any Traffic	ssh https	accept	None
3	0	Stealth	Any	fwsingapore	Any Traffic	Any	drop	Log
4	0	User Auth	Any	webSingapore	Any Traffic	http	User Auth	Log
5	0	Partner City	net_singapore net_rome	net_rome net_singapore	rome_singapore	http	accept	Log
6	0	Network Traffic	net_singapore net_sydney	Any	Any Traffic	http dns icmp-proto ftp https	accept	Log
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log

- A. Rule 4
- B. Rule 6
- C. Rule 3
- D. Rule 5



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

Which tool CANNOT be launched from SmartUpdate R77?



<https://vceplus.com/>

- A. IP Appliance Voyager
- B. snapshot
- C. GAIa WebUI
- D. cpinfo

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 143

Which of the following is a hash algorithm?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 144

Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 145

You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities sh you do first?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 146

What must a Security Administrator do to comply with a management requirement to log all traffic accepted through the perimeter Security Gateway?

- A. In **Global Properties > Reporting Tools** check the box **Enable tracking all rules** (including rules marked as **None** in the **Track** column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting. B. Install the **View Implicit Rules** package using SmartUpdate.
- C. Define two log servers on the R77 Gateway object. **Log Implied Rules** on the first log server. Enable **Log Rule Base** on the second log server. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits. D. Check the **Log Implied Rules Globally** box on the R77 Gateway object.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147

What is the appropriate default Gaia Portal address?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:



QUESTION 148

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149

Match the following commands to their correct function. Each command has one function only listed.

Command	Function
C1 cp_admin_convert	F1: export and import different revisions of the database.
C2 cpea_client	F2: export and import policy package
C3 cp_merge	F3: transfer Log data to an external database.
C4 cpwd_admin	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in cpconfig to SmartDashboard.

- A. C1>F6; C2>F4; C3>F2; C4>F5
B. C1>F2; C2>F1; C3>F6; C4>F4
C. C1>F2; C2>F4; C3>F1; C4>F5
D. C1>F4; C2>F6; C3>F3; C4>F5



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 150

Which of the following is NOT an option for internal network definition of Anti-spoofing?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 151

MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How do you apply the license?

- A. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- B. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- C. Using the remote Gateway's IP address, and applying the license locally with command `cplic put`.
- D. Using each of the Gateway's IP addresses, and applying the licenses on the Security Management Server with the command `cprlic put`.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 152

A digital signature:

- A. Guarantees the authenticity and integrity of a message.
- B. Automatically exchanges shared keys.
- C. Decrypts data to its original form.
- D. Provides a secure key exchange mechanism over the Internet.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 153

According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

- A. Interoperable Device

- B. Network Node
- C. Externally managed gateway
- D. Gateway

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 154

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 155

When launching SmartDashboard, what information is required to log into R77?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 156

A Cleanup rule:

- A. logs connections that would otherwise be dropped without logging by default.
- B. drops packets without logging connections that would otherwise be dropped and logged by default.
- C. logs connections that would otherwise be accepted without logging by default.
- D. drops packets without logging connections that would otherwise be accepted and logged by default.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

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 159

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 160

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 161

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 162

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 163

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

- A. Run `fwm dbexport -1 filename`. Restore the database. Then, run `fwm dbimport -1 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 164

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 165

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 166

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 167

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?



<https://vceplus.com/>

- 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 168

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 169

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 170

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 171

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 172

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 173

What is the Manual Client Authentication TELNET port?

- A. 23
- B. 264C. 900
- D. 259

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 174

Jennifer McHenry 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 McHenry access network destinations. Select accept as the Action. 4) Install policy.
- Ms McHenry 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 175

How many packets does the IKE exchange use for Phase 1 Main Mode?

- A. 12
- B. 1C. 3
- D. 6

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 176

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 177

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 178

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 179

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 180

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.

D.

Connections to and from the specified target are blocked without the need to change the Security Policy.
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 181

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 182

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 183

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. 18184C. 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 184

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 185

The CDT utility supports which of the following?

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

D.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 186

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

Explanation/Reference:



QUESTION 187

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 188

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 189

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.
- 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 190

What are the three components for Check Point Capsule?

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

D.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 191

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

Explanation/Reference:



QUESTION 192

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:

<https://vceplus.com/>

QUESTION 193

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 194

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



<https://vceplus.com/>

- A. Any size
- 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 195

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 196

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

Explanation/Reference:

QUESTION 197

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 198

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 199

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 200

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 201

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm

QUESTION 202

You want to store the GAIa configuration in a file for later reference. What command should you use?

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

D. save configuration <filename>

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk102234

QUESTION 203

Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 204

From SecureXL perspective, what are the tree paths of traffic flow:

- A. Initial Path; Medium Path; Accelerated Path
- B. Layer Path; Blade Path; Rule Path
- C. Firewall Path; Accept Path; Drop Path
- D. Firewall Path; Accelerated Path; Medium Path

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 205

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 206

R80.10 management server can manage gateways with which versions installed?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk113113

QUESTION 207

You want to verify if there are unsaved changes in GAIa that will be lost with a reboot. What command can be used?

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

D. show config-state

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 208

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

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

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm

QUESTION 209

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- A. Symmetric routing
- B. Failovers
- C. Asymmetric routing
- D. Anti-Spoofing

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 210

What are the steps to configure the HTTPS Inspection Policy?

- A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
- B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
- C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
- D. Go to Application&url filtering blade > Https Inspection > Policy

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 211

What is the difference between SSL VPN and IPSec VPN?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Mobile_Access_WebAdmin/83586.htm

QUESTION 212

Which statement is NOT TRUE about Delta synchronization?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7288.htm

QUESTION 213

Under which file is the proxy arp configuration stored?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76SP.10/CP_R76SP.10_Security_System_AdministrationGuide/105233.htm

QUESTION 214

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 215

SmartEvent does NOT use which of the following procedures to identify events:

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEvent_AdminGuide/17401.htm

QUESTION 216

John is using Management HA. Which Smartcenter should be connected to for making changes?

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 217

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 218

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 219

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 220

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 221

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 222

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 223

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?



<https://vceplus.com/>

- 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 224

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 225

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 226

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 227

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 228

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 229

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 230

Fill in the blank: An LDAP server holds one or more _____.

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

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 231

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 232

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 233

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 234

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 235

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: C

Section: (none)

Explanation



Explanation/Reference:

QUESTION 236

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 237

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 238

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 239

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 240

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 241

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 242

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 243

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 244

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 245

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:



<https://vceplus.com/>

