156-215.80.exam.252q

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

156-215.80

Check Point Certified Security Administrator R80

Exam A

QUESTION 1
Which of the following ClusterXL modes uses a non-unicast MAC address for the cluster IP address.

A. High Availability
B. Load Sharing Multicast
C. Load Sharing Pivot
D. Master/Backup

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation : ClusterXL uses the Multicast mechanism to associate the virtual cluster IP addresses with all cluster members. By binding these IP addresses to a Multicast MAC address, it ensures that all packets sent to the cluster, acting as a gateway, will reach all members in the cluster.

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

QUESTION 2
Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) ___________ Server.

A. NT domain

B. SMTP
C. LDAP
D. SecurID

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

QUESTION 3
Which of the following is **NOT** a component of a Distinguished Name?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 4
What are the three authentication methods for SIC?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Secure Internal Communication (SIC)

Secure Internal Communication (SIC) lets Check Point platforms and products authenticate with each other. The SIC procedure creates a trusted status between gateways, management servers and other Check Point components. SIC is required to install polices on gateways and to send logs between gateways and management servers.

These security measures make sure of the safety of SIC:

▪ Certificates for *authentication*

▪ Standards-based SSL for the creation of the secure channel ▪
3DES for *encryption*

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

QUESTION 5

You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 6

What is the order of NAT priorities?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation: The order of NAT priorities is:

1. Static NAT
2. IP Pool NAT
3. Hide NAT

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

QUESTION 7
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

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

Correct Answer: B
Section: (none)
Explanation

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

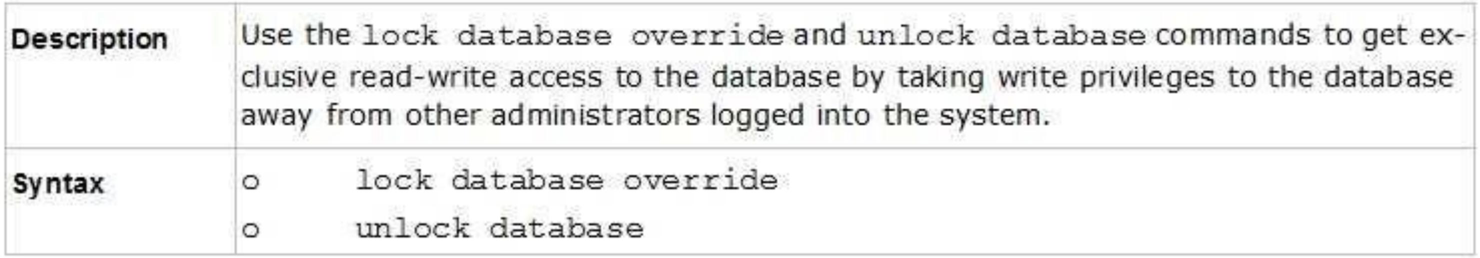
QUESTION 8
Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

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

Correct Answer: D

Section: (none)
Explanation

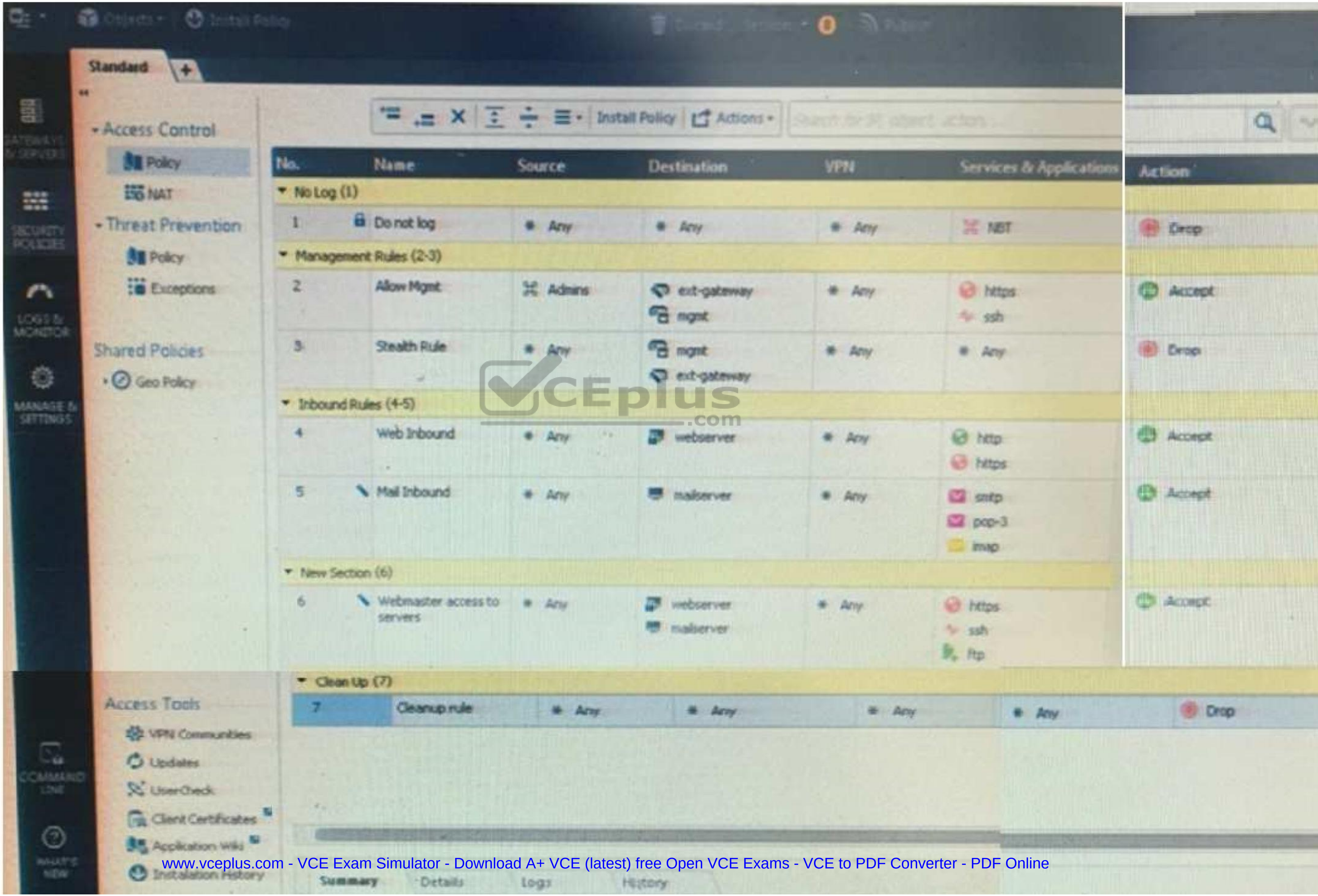
Explanation/Reference:
Explanation: Use the *database* feature to obtain the configuration lock. The database feature has two commands: ▪
`lock database [override].`
▪ `unlock database`
The commands do the same thing: obtain the configuration lock from another administrator.



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

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

QUESTION 9
Examine the following Rule Base.



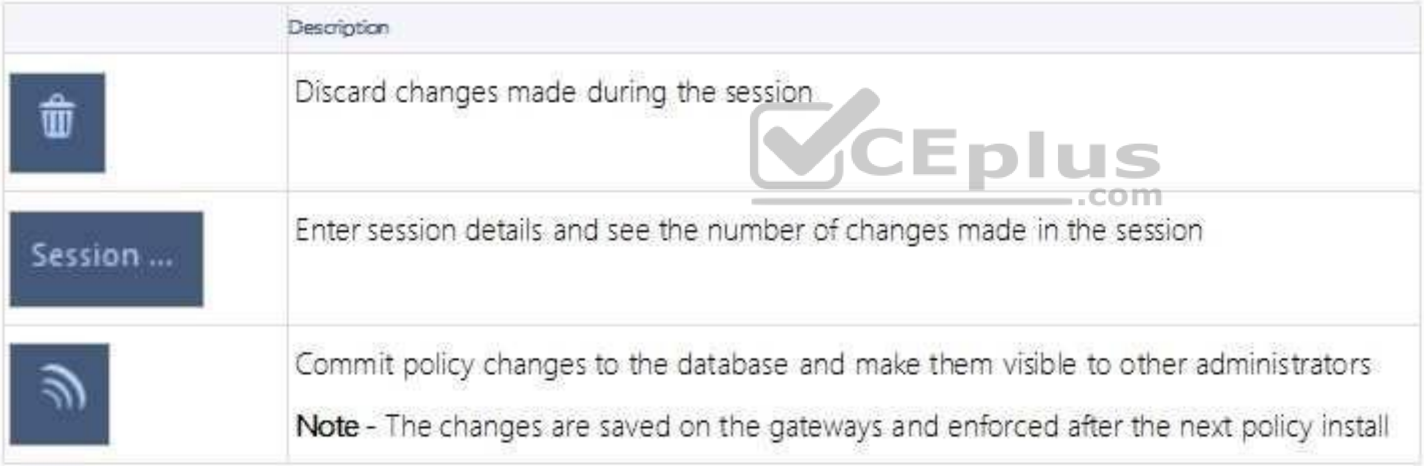
No.	Name	Source	Destination	VPN	Services & Applications	Action
No Log (1)						
1	Do not log	Any	Any	Any	NBT	Drop
Management Rules (2-3)						
2	Allow Mgmt	Admins	ext-gateway mgmt	Any	https ssh	Accept
3	Stealth Rule	Any	mgmt ext-gateway	Any	Any	Drop
Inbound Rules (4-5)						
4	Web Inbound	Any	webserver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

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

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

Correct Answer: D
Section: (none)
Explanation

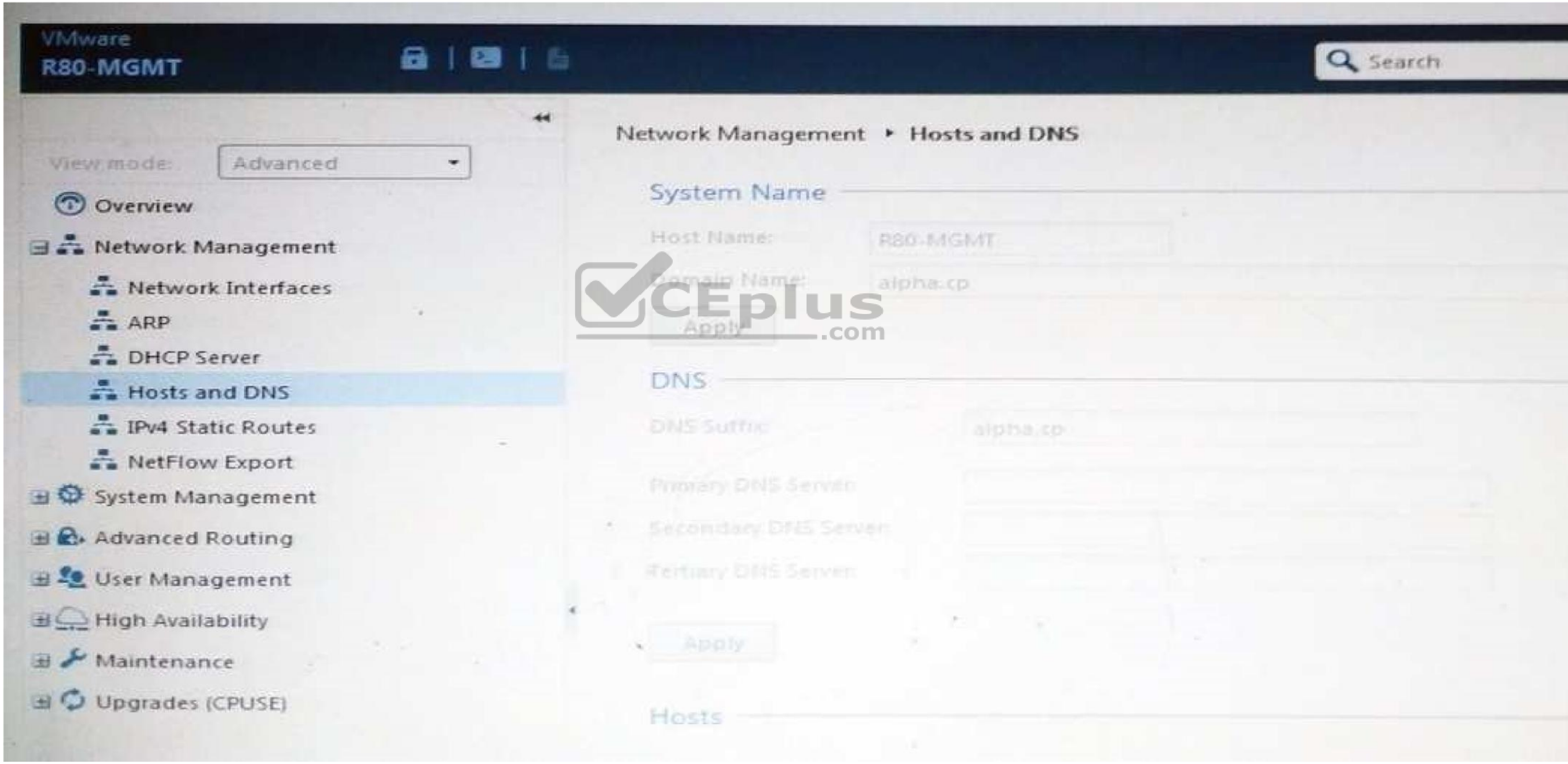
Explanation/Reference:
Explantation: On top of the print screen there is a number "8" which consists for the number of changes made and not saved.
Session Management Toolbar (top of SmartConsole)



	Description
🗑	Discard changes made during the session
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 10
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?



Network Management ▸ Hosts and DNS

System Name

Host Name: R80-MGMT

Domain Name: alpha.cp

Apply

DNS

DNS Suffix: alpha.cp

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

Apply

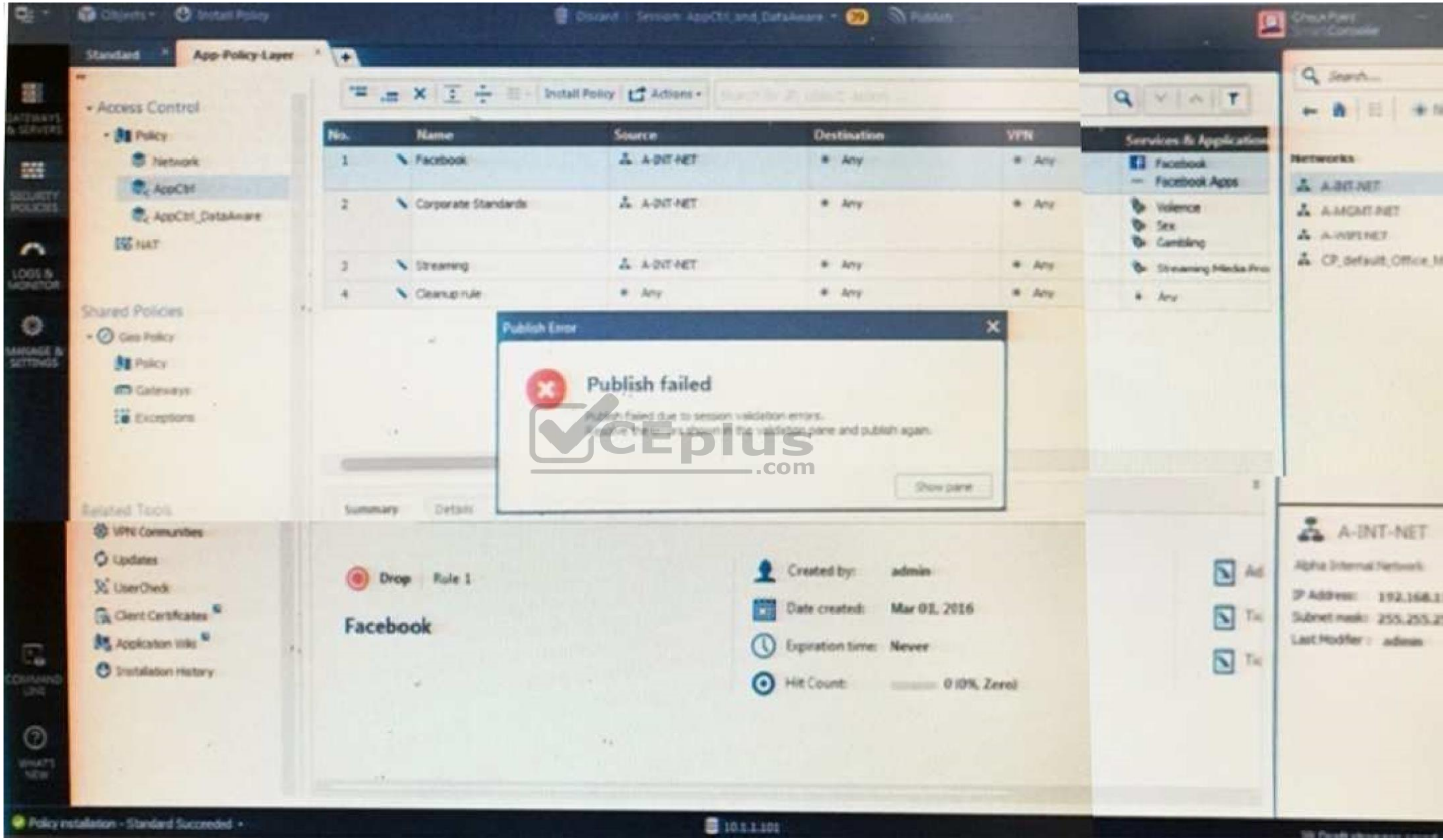
Hosts

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 11
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?



No.	Name	Source	Destination	VPN	Services & Applications
1	Facebook	A-INT-NET	Any	Any	Facebook Facebook Apps
2	Corporate Standards	A-INT-NET	Any	Any	Violence Sex Gambling
3	Streaming	A-INT-NET	Any	Any	Streaming Media Pro
4	Cleanup rule	Any	Any	Any	Any

Publish Error

Publish failed

Publish failed due to session validation errors.
Resolve the errors shown in the validation pane and publish again.

Drop Rule 1

Facebook

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

A-INT-NET
A-MGMT-NET
A-WIFI-NET
CP_default_Office_M

A-INT-NET
Alpha Internal Network
IP Address: 192.168.1.
Subnet mask: 255.255.2
Last Modifier: admin

Policy installation - Standard Succeeded
10.1.1.101

A. The Log and Monitor section in SmartConsole
B. The Validations section in SmartConsole
C. The Objects section in SmartConsoleD. 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 12
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 13
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 14
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 15
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 16
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 17
By default, which port does the WebUI listen on?

A. 80
B. 4434C. 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 18
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 19
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 20
What is the default time length that Hit Count Data is kept?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Keep Hit Count data up to - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.

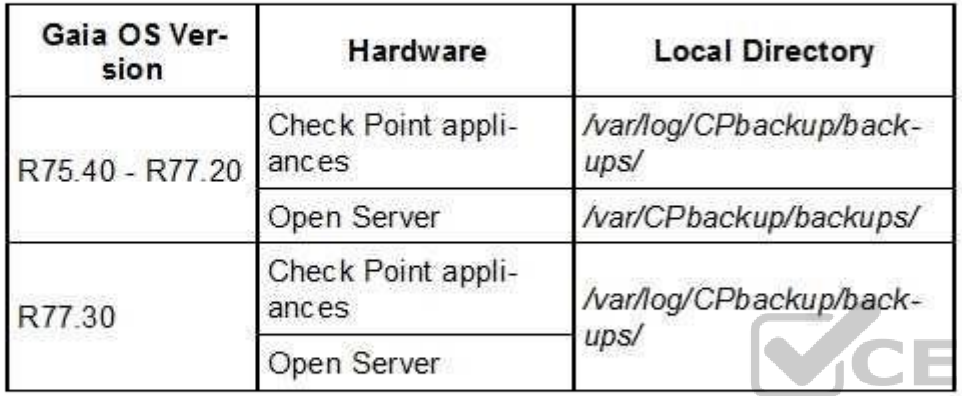
Reference: http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?HashKey=1479584563_6f823c8ea1514609148aa4fec5425db2&xtn=.pdf

QUESTION 21
Choose the Best place to find a Security Management Server backup file named `backup_fw`, on a Check Point Appliance.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration.
The configuration is saved to a *.tgz* file in the following directory:



Gaia OS Version	Hardware	Local Directory
R75.40 - R77.20	Check Point appliances	*/var/log/CPbackup/backups/*
	Open Server	*/var/CPbackup/backups/*
R77.30	Check Point appliances	*/var/log/CPbackup/backups/*
	Open Server	

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

QUESTION 22
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 23
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 24
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 25
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 26
Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

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

Correct Answer: C
Section: (none)
Explanation

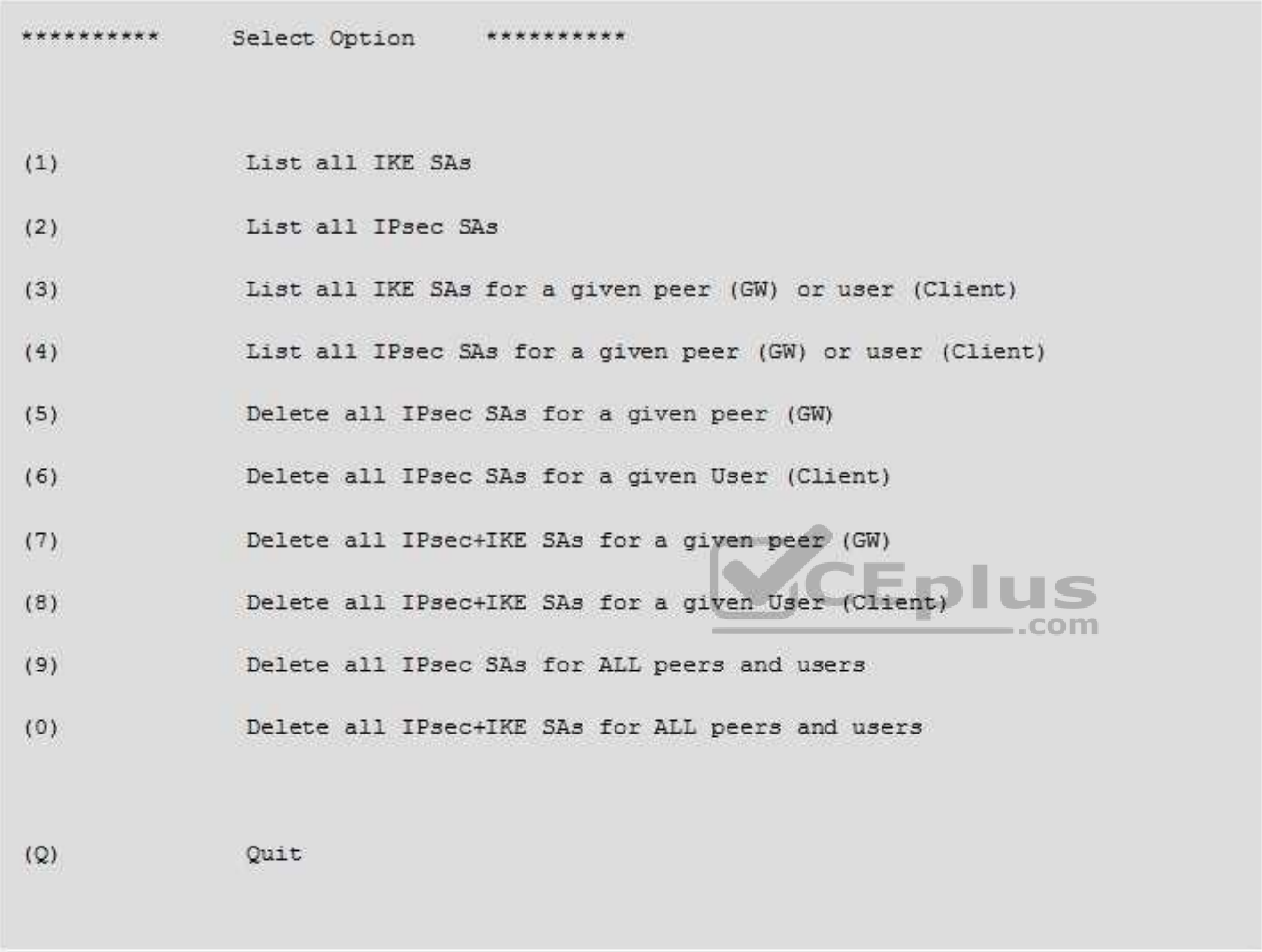
Explanation/Reference:
Explanation: One for Security Management Server and the other one for the Security Gateway.

QUESTION 27
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 28
Which of the following is **NOT** an authentication scheme used for accounts created through SmartConsole?

A. Security questions
B. Check Point password

C. SecurID
D. RADIUS

Correct Answer: A
Section: (none)
Explanation

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

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

QUESTION 29
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 30

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 31

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

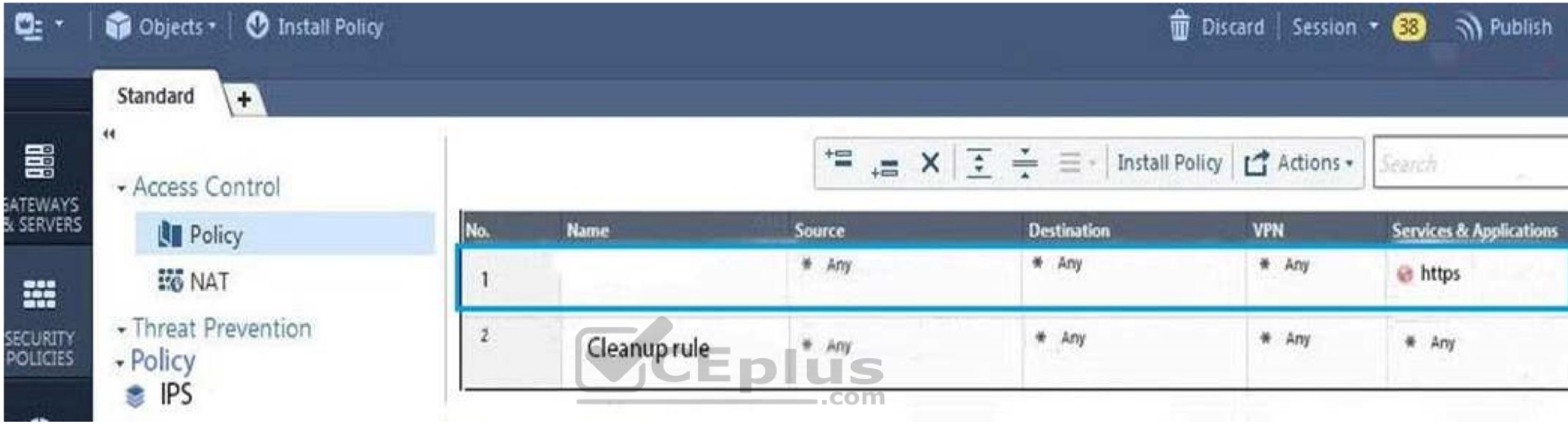
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 32

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



No.	Name	Source	Destination	VPN	Services & Applications
1		* Any	* Any	* Any	https
2	Cleanup rule	* Any	* Any	* Any	* Any

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

A. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if implicit Drop Rule drops the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer.

B. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to IPS layer and then after accepting the packet it passes to Threat Prevention layer

C. A packet arrives at the gateway, it is checked against the rules in the networks policy layer and then if there is any rule which accepts the packet, it comes next to Threat Prevention layer and then after accepting the packet it passes to IPS layer.

D. A packet arrives at the gateway, it is checked against the rules in IPS policy layer and then it comes next to the Network policy layer and then after accepting the packet it passes to Threat Prevention layer.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation: To simplify Policy management, R80 organizes the policy into Policy Layers. A layer is a set of rules, or a Rule Base.

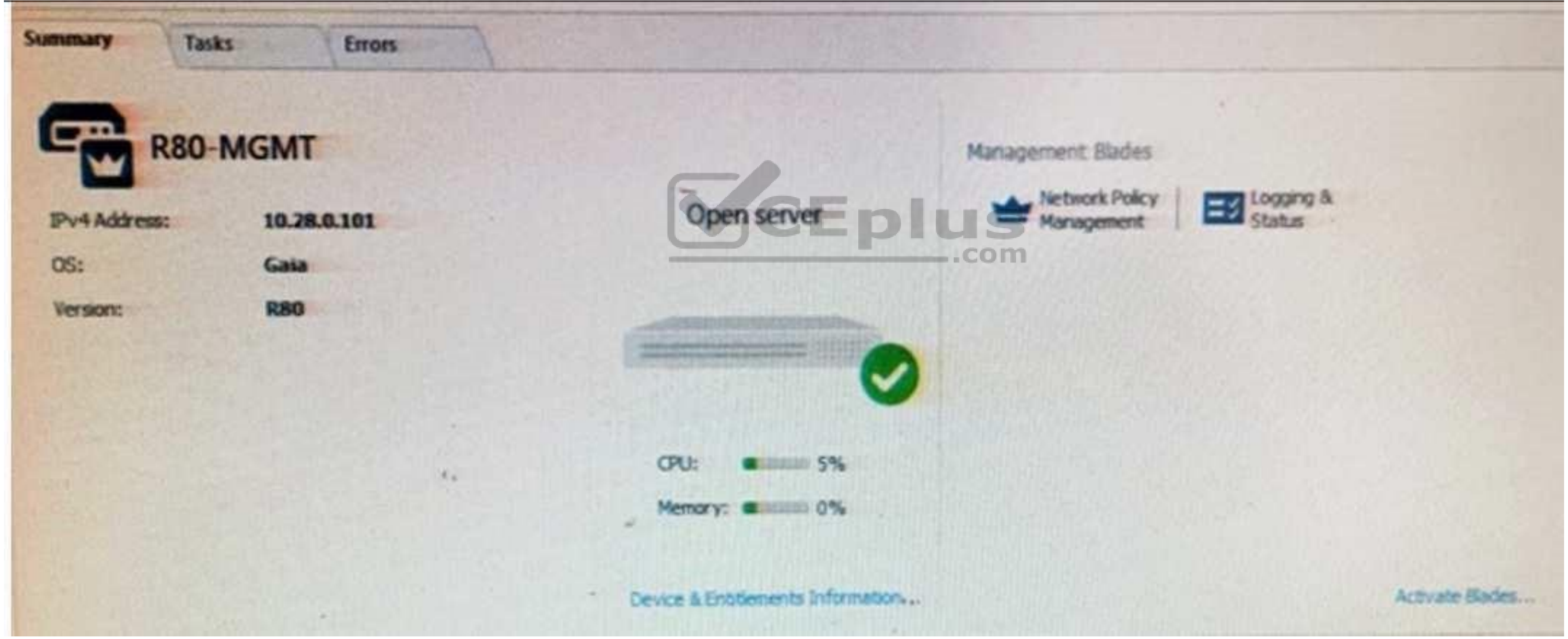
For example, when you upgrade to R80 from earlier versions:

- Gateways that have the Firewall and the Application Control Software Blades enabled will have their Access Control Policy split into two ordered layers: Network and Applications.
  When the gateway matches a rule in a layer, it starts to evaluate the rules in the next layer.
- Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.
  All layers are evaluated in parallel

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

QUESTION 33

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'?



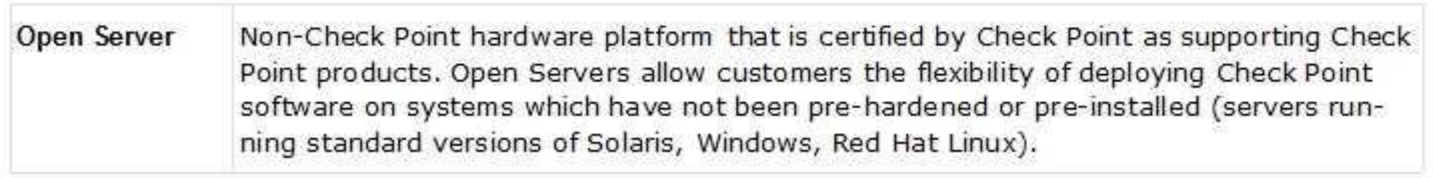
IPv4 Address: 10.28.0.101
OS: Gaia
Version: R80
CPU: 5%
Memory: 0%

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 34
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 35
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 36

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

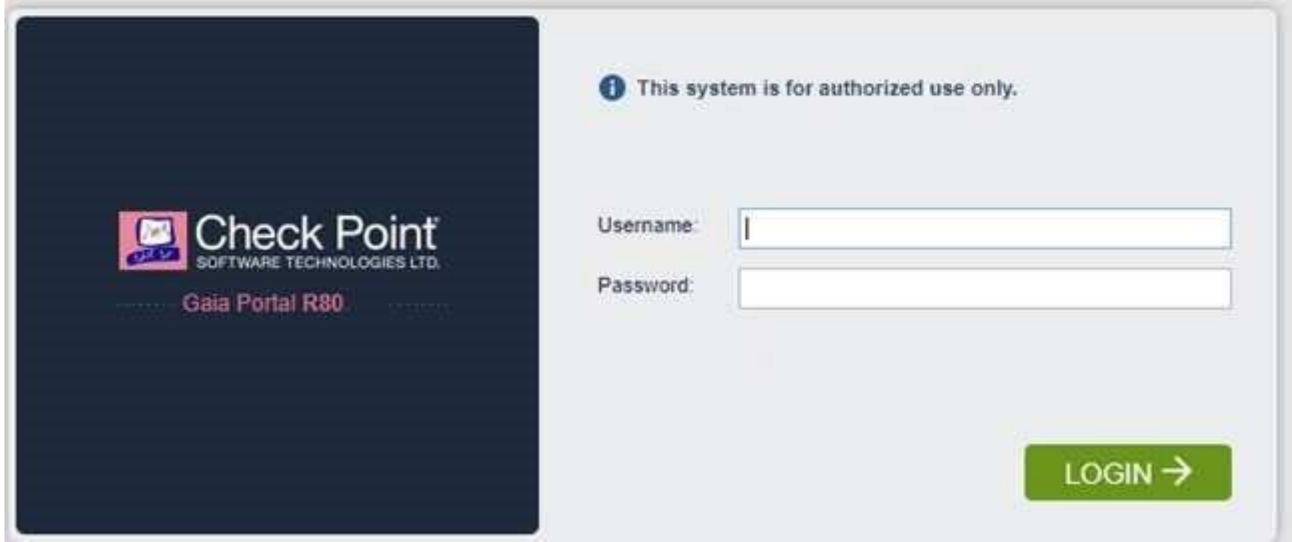
Explanation/Reference:

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 37

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



This system is for authorized use only.

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

B. `set Gaia-portal <new port number>`

C. `set Gaia-portal https-port <new port number>`

D. `set web https-port <new port number>`

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 'httpd:ssl_port' /config/db/initial Reference:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482

QUESTION 38

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 39

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 40

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 41

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 42

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 43
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 44
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?

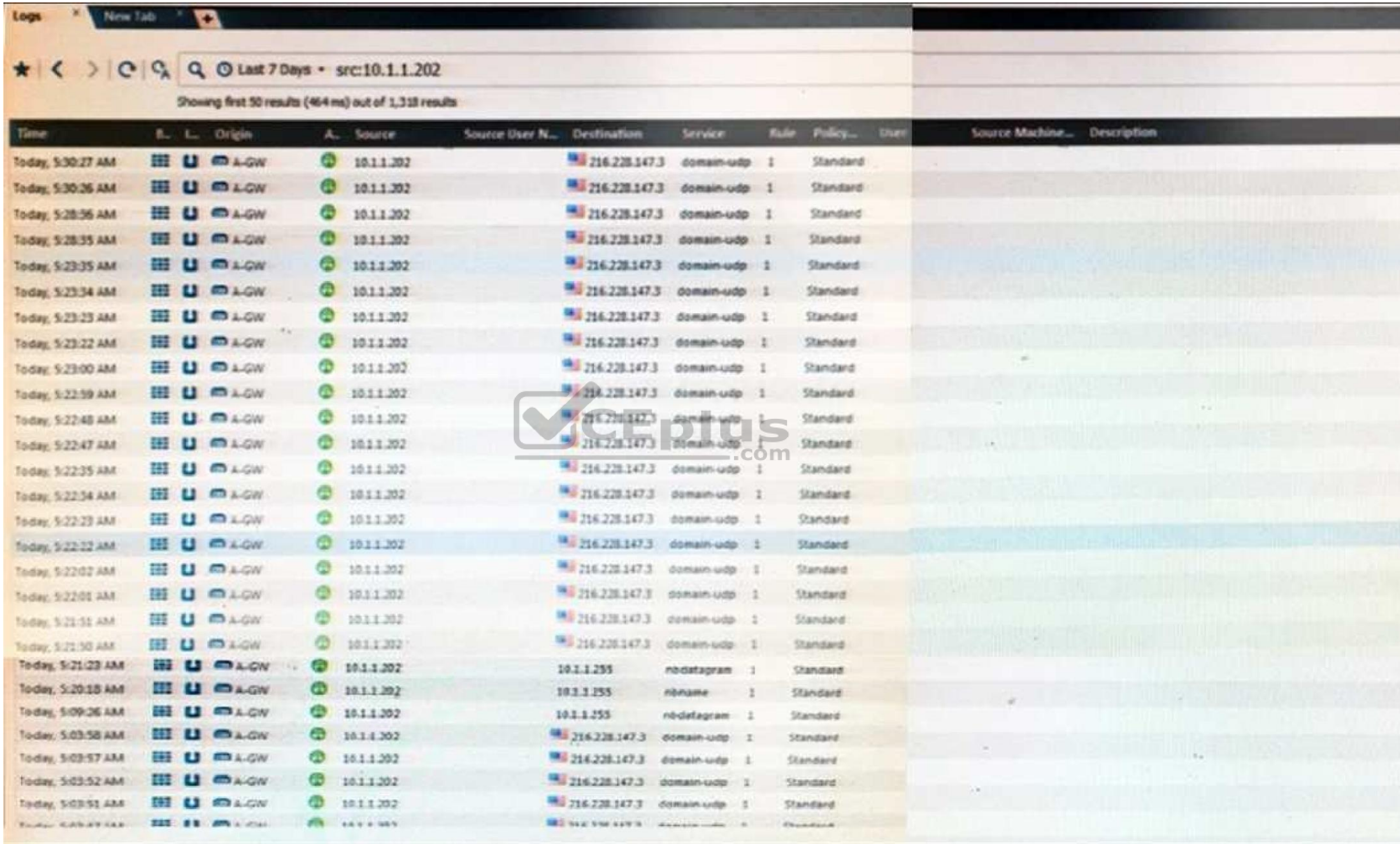
A. `cpconfig`
B. `fw ctl pstat`
C. `cpview`
D. `fw ctl multik stat`

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 45

The following graphic shows:



Last 7 Days • src:10.1.1.202

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

Time	B...	L...	Origin	A...	Source	Source User N...	Destination	Service	Rule	Policy...	User	Source Machine...	Description
Today, 5:30:27 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:30:26 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:56 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:55 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:35 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:34 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:23 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:22 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:00 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:59 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:48 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:47 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:35 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:34 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:23 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:22 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:02 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:01 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:51 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:50 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:23 AM	▦	U	A-GW	●	10.1.1.202		10.1.1.255	nbdatagram	1	Standard			
Today, 5:20:18 AM	▦	U	A-GW	●	10.1.1.202		10.1.1.255	nbname	1	Standard			
Today, 5:09:26 AM	▦	U	A-GW	●	10.1.1.202		10.1.1.255	nbdatagram	1	Standard			
Today, 5:03:58 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:57 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:52 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:51 AM	▦	U	A-GW	●	10.1.1.202		216.228.147.3	domain-udp	1	Standard			
[illegible]	▦	U	A-GW	●	[illegible]		[illegible]	[illegible]	[illegible]	[illegible]			

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 46
In R80, Unified Policy is a combination of

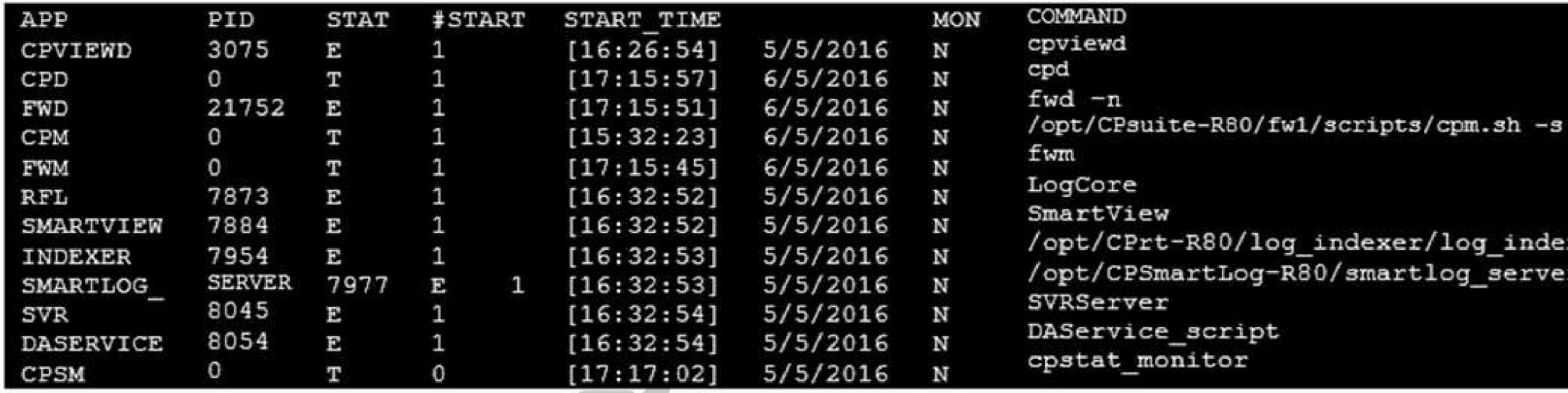
A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.
B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security Policy and Threat Prevention 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 47

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



```
APP          PID      STAT    #START    START_TIME               MON    COMMAND
CPVIEWD      3075     E       1         [16:26:54]  5/5/2016     N      cpviewd
CPD          0        T       1         [17:15:57]  6/5/2016     N      cpd
FWD          21752    E       1         [17:15:51]  6/5/2016     N      fwd -n
CPM          0        T       1         [15:32:23]  6/5/2016     N      /opt/CPsuite-R80/fw1/scripts/cpm.sh -s
FWM          0        T       1         [17:15:45]  6/5/2016     N      fwm
RFL          7873     E       1         [16:32:52]  5/5/2016     N      LogCore
SMARTVIEW    7884     E       1         [16:32:52]  5/5/2016     N      SmartView
INDEXER      7954     E       1         [16:32:53]  5/5/2016     N      /opt/CPrt-R80/log_indexer/log_inde
SMARTLOG_    SERVER   7977    E     1   [16:32:53]  5/5/2016     N      /opt/CPSmartLog-R80/smartlog_serve
SVR          8045     E       1         [16:32:54]  5/5/2016     N      SVRServer
DASERVICE    8054     E       1         [16:32:54]  5/5/2016     N      DAService_script
CPSM         0        T       0         [17:17:02]  5/5/2016     N      cpstat_monitor
```

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

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

Correct Answer: C
Section: (none)
Explanation

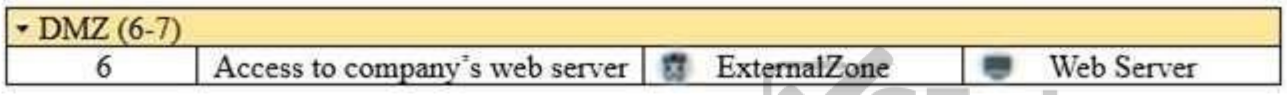
Explanation/Reference:
The correct answer would be FWM (is the process making available communication between SmartConsole applications and Security Management Server.).
STATE is T (Terminate = Down)
Explanation :
Symptoms

- SmartDashboard fails to connect to the Security Management server.

1. Verify if the FWM process is running. To do this, run the command:
[Expert@HostName:0]# ps -aux | grep fwm
2. If the FWM process is not running, then try force-starting the process with the following command:
[Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"

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

QUESTION 48
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 49
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 50
What are the two high availability modes?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

- **Load Sharing Multicast Mode** ▪
Load Sharing Unicast Mode
- **New High Availability Mode**
- **High Availability Legacy Mode**

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

QUESTION 51
Fill in the blank: The R80 feature ________ permits blocking specific IP addresses for a specified time period.

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 52
Which Threat Prevention Software Blade provides comprehensive against malicious and unwanted network traffic, focusing on application and server vulnerabilities?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: The IPS Software Blade provides a complete Intrusion Prevention System security solution, providing comprehensive network protection against malicious and unwanted network traffic, including:

- Malware attacks
- Dos and DDoS attacks
- Application and server vulnerabilities
- Insider threats
- Unwanted application traffic, including IM and P2P

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

QUESTION 53
What is the purpose of Captive Portal?

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

Correct Answer: C
Section: (none)
Explanation

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

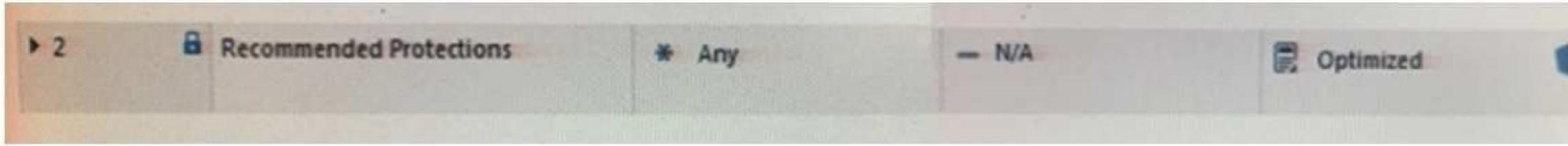
QUESTION 54
While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?

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

Correct Answer: B
Section: (none)
Explanation

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

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



QUESTION 55
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 56
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

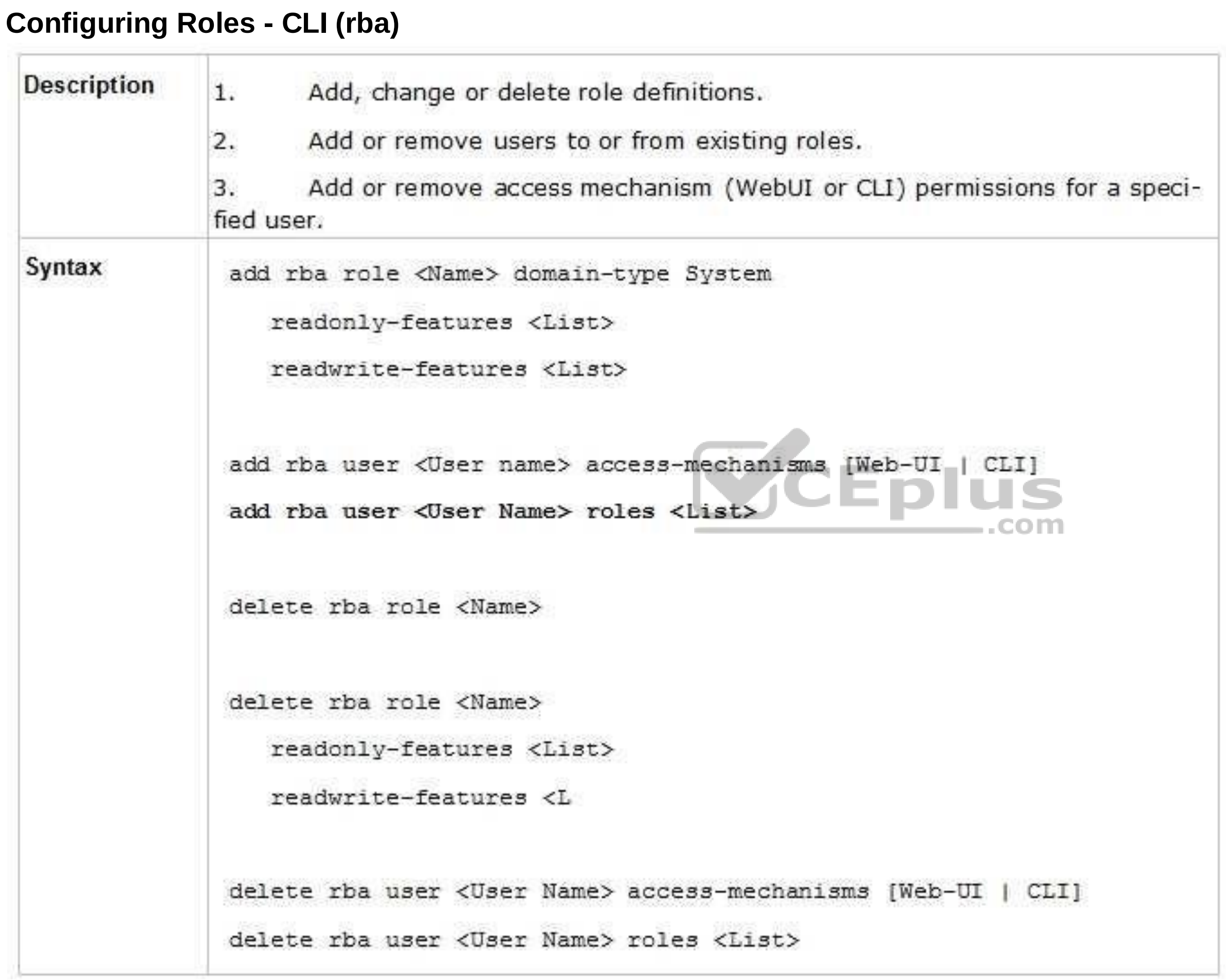
Explanation/Reference:

QUESTION 57
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)

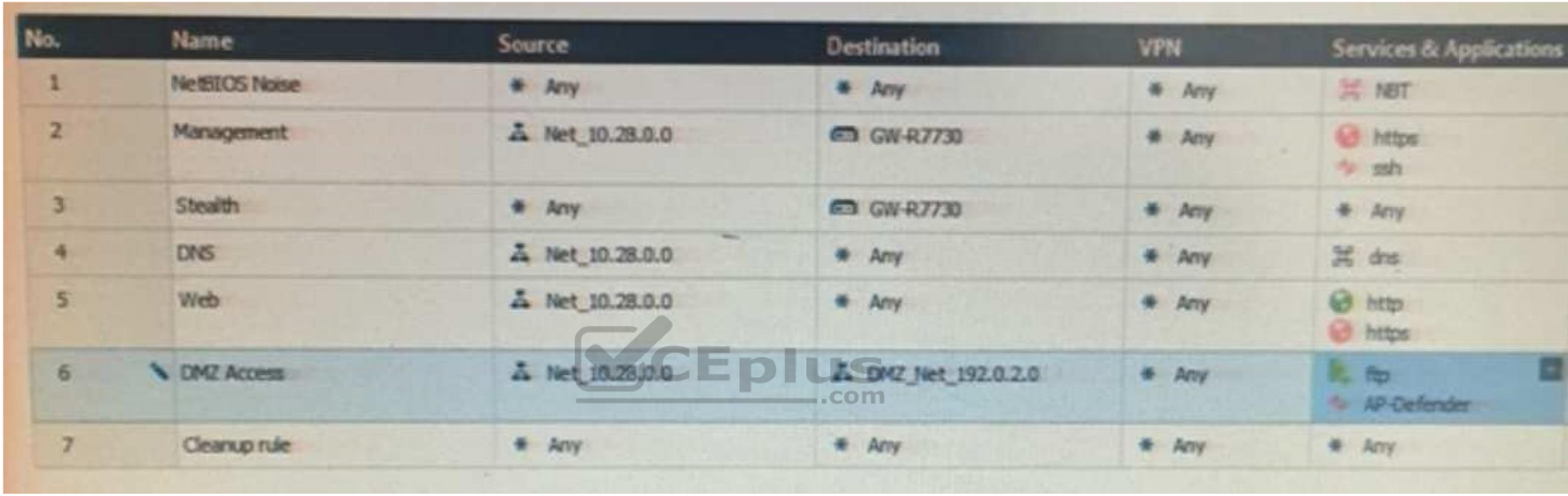
Description	1. Add, change or delete role definitions. 2. Add or remove users to or from existing roles. 3. Add or remove access mechanism (WebUI or CLI) permissions for a specified user.

Syntax	`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>`

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73101.htm **QUESTION 58**

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	NBT
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 59
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

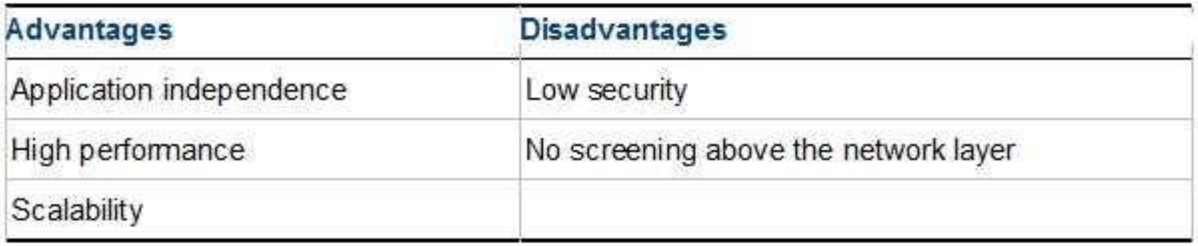
Explanation/Reference:

QUESTION 60
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

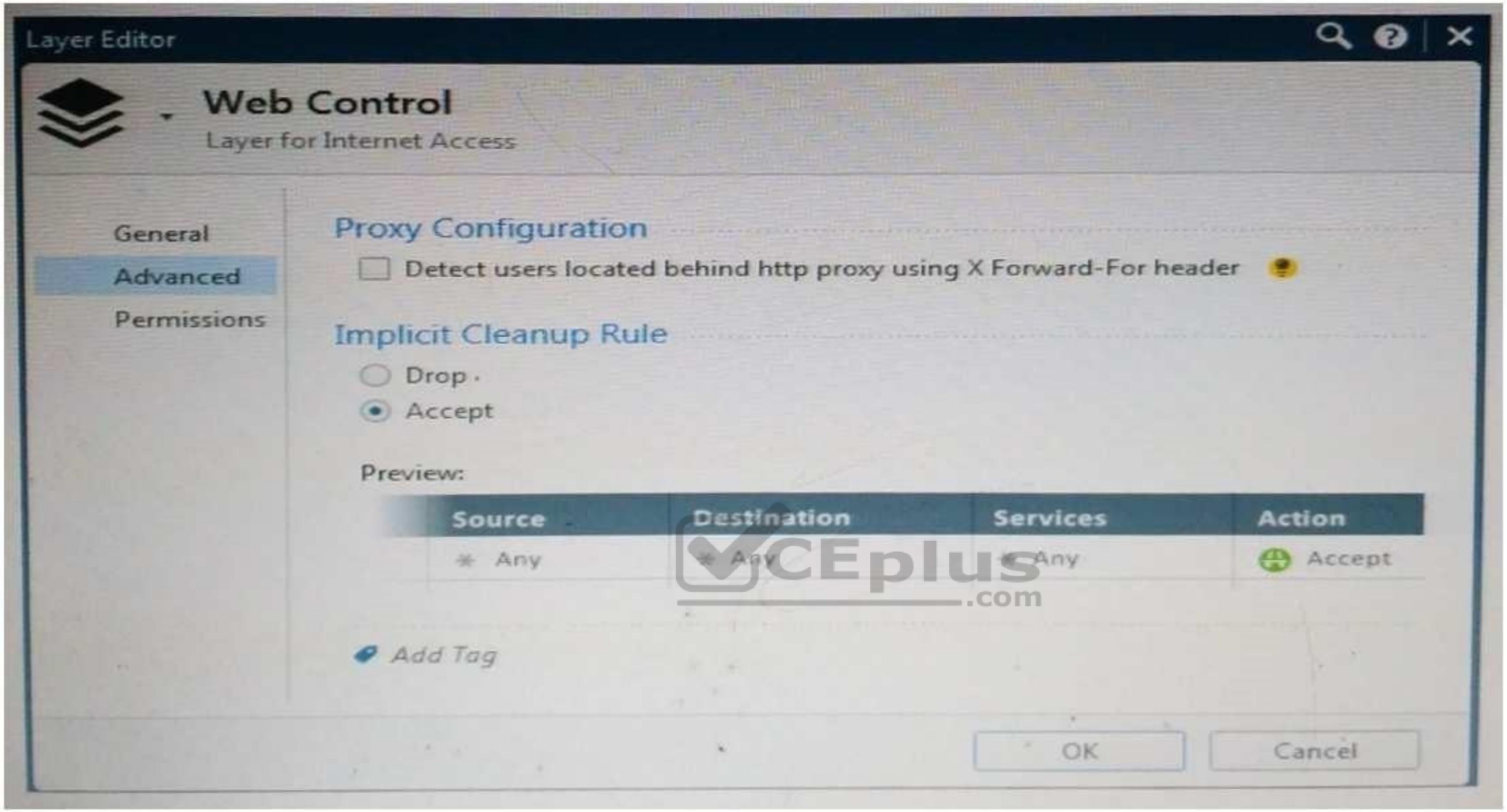
QUESTION 61
In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

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 62
Web Control Layer has been set up using the settings in the following dialogue:



Web Control

Layer for Internet Access

Proxy Configuration

□ Detect users located behind http proxy using X Forward-For header

Implicit Cleanup Rule

○ Drop

● Accept

Preview:

Source	Destination	Services	Action
Any	Any	Any	Accept

Consider the following policy and select the BEST answer.

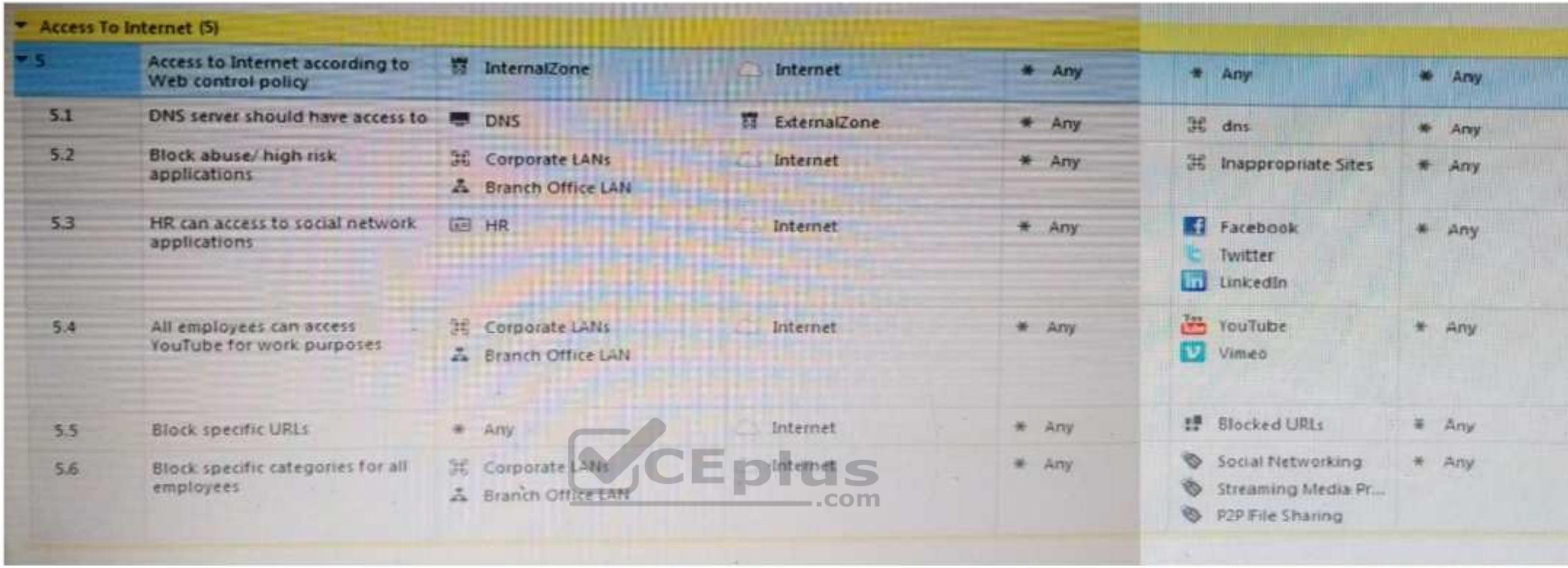
A. Traffic that does not match any rule in the subpolicy is dropped.

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, expect 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 63

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 64

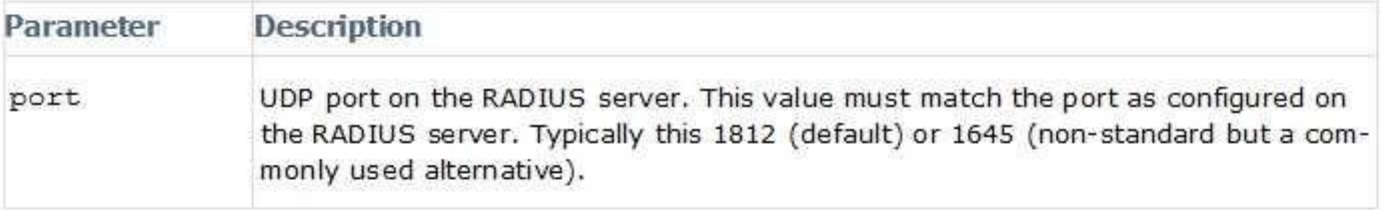
Fill in the blank: RADIUS protocol uses ______ to communicate with the gateway.

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 65

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 66

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 67
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 68
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?

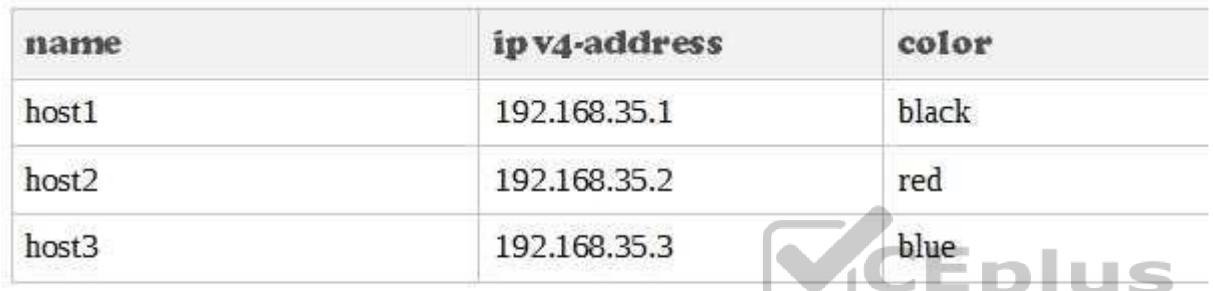
A. Create a text-file with `mgmt_cli` script that creates all objects and policies. Open the file in SmartConsole Command Line to run it.
B. Create a text-file with Gaia CLI -commands in order to create all objects and policies. Run the file in CLISH with command `load configuration`.
C. Create a text-file 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:



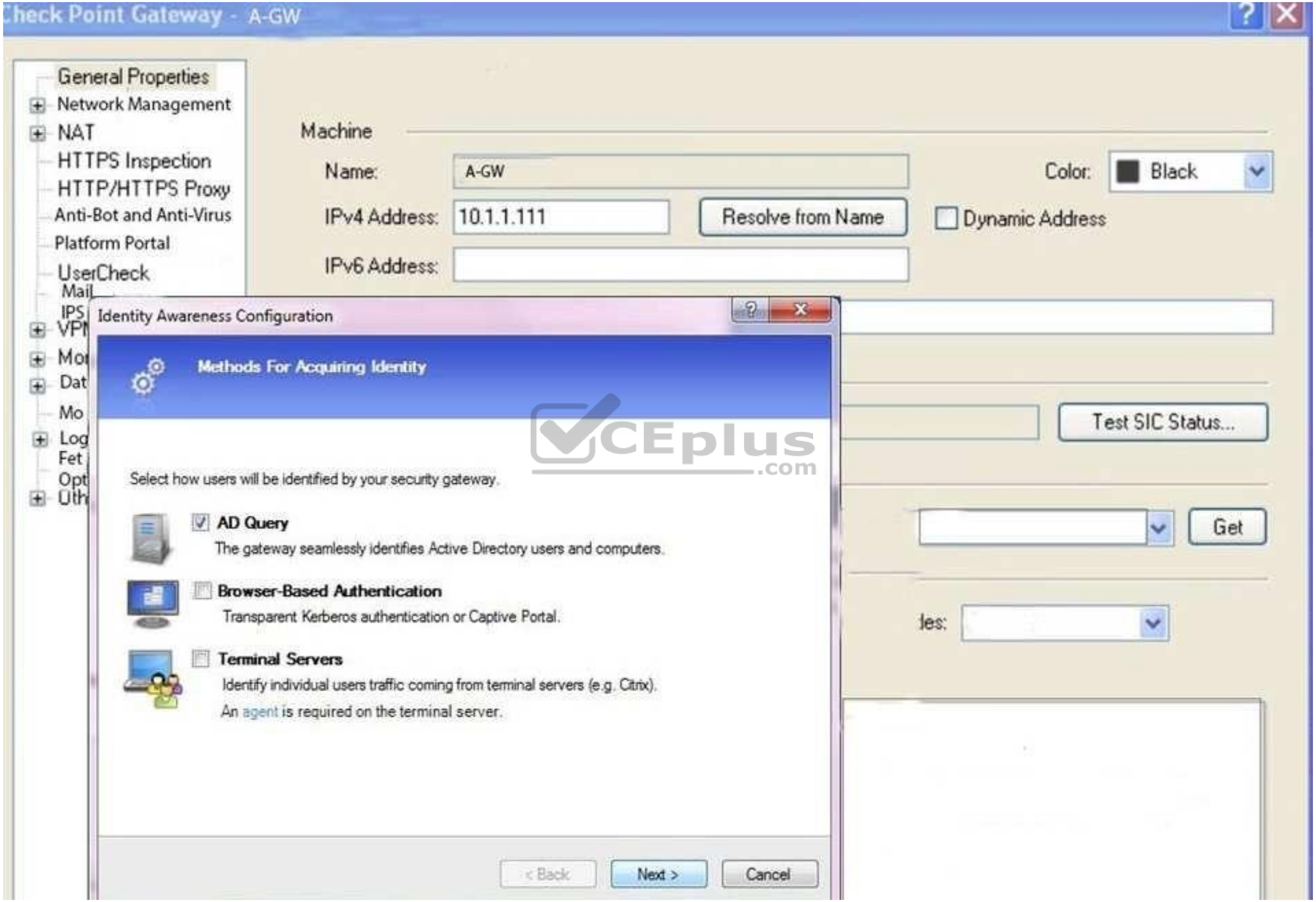
name	ipv4-address	color
host1	192.168.35.1	black
host2	192.168.35.2	red
host3	192.168.35.3	blue

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

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

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

QUESTION 69
On the following picture an administrator configures Identity Awareness:



Name: A-GW

Color: Black

IPv4 Address: 10.1.1.111

□ 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.

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

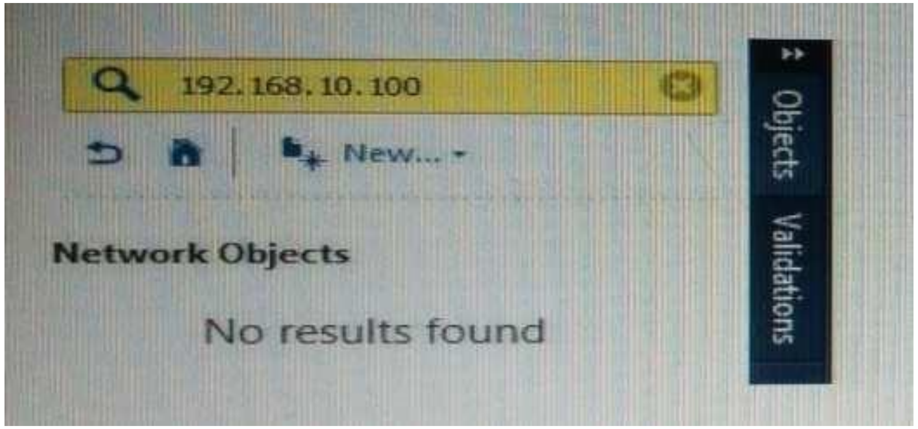
A. Kerberos SSO which will be working for Active Directory integration
B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user
C. Obligatory usage of Captive Portal
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 70
What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.



192.168.10.100

Network Objects

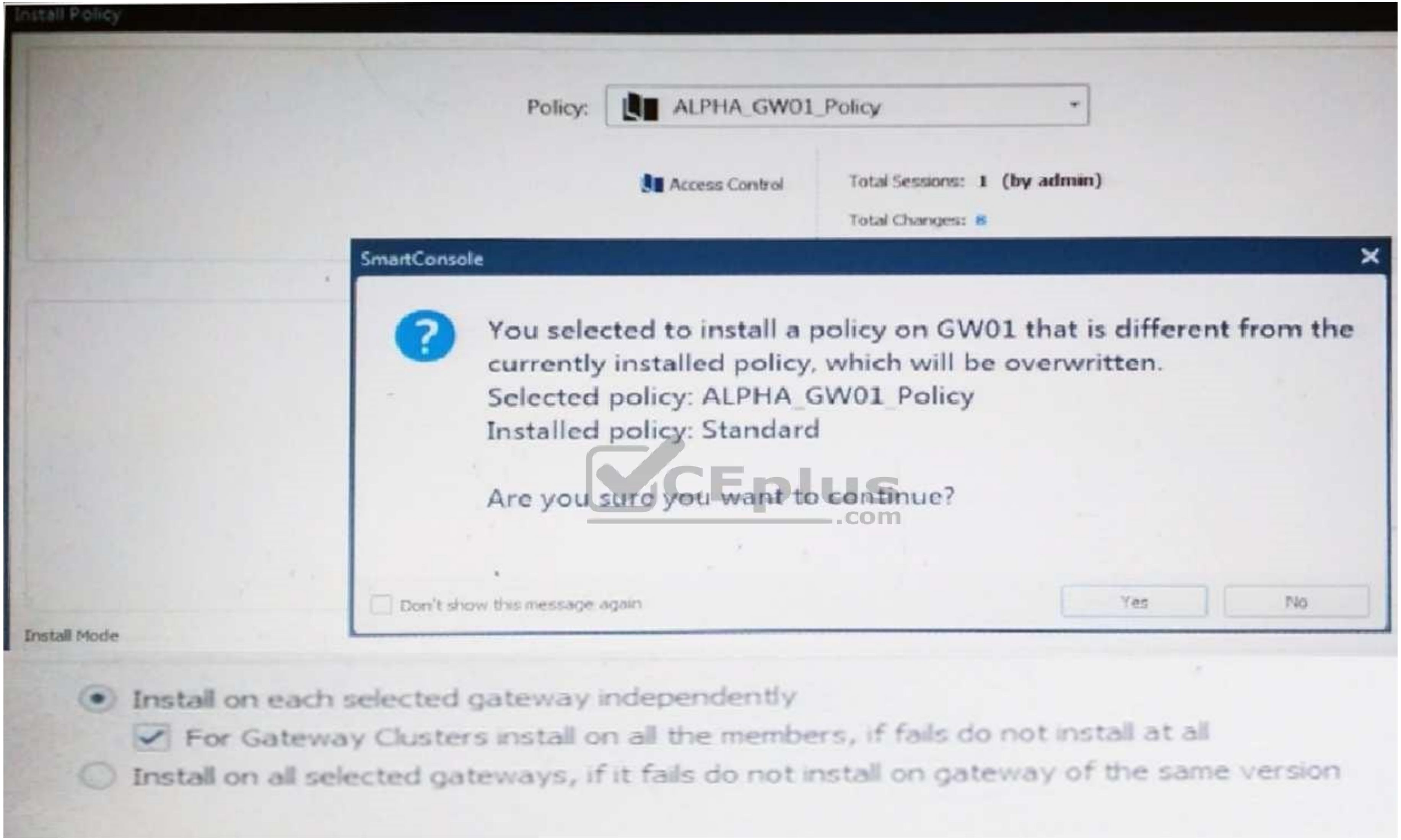
No results found

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 71
Why would an administrator see the message below?



Install Policy

Policy: ALPHA_GW01_Policy

Total Sessions: 1 (by admin)

Total Changes: 8

SmartConsole

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

Are you sure you want to continue?

□ Don't show this message again

Install Mode

● Install on each selected gateway independently

☑ For Gateway Clusters install on all the members, if fails do not install at all

○ Install on all selected gateways, if it fails do not install on gateway of the same version

A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.

B. A new Policy Package created on the Management is going to be installed to the existing Gateway.

C. A new Policy Package created on the Gateway is going to be installed on the existing Management.

D. A new Policy Package created on the Gateway and transferred to the management will be overwritten 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 72
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 73
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 74
In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

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

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 75
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 76
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 77
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 78

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 79

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 80
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 81
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 82

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 83

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 84
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 85
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 86
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 87

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 88

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 89

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 90
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:
Exlantion: 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 91
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 (*lv_current*) disk partition. This includes Check Point products, configuration, and operating system.
Starting in **R77.10**, exporting an image from one machine and importing that image on another machine of the same type is supported.
The *log* partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be saved.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902

QUESTION 92
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.

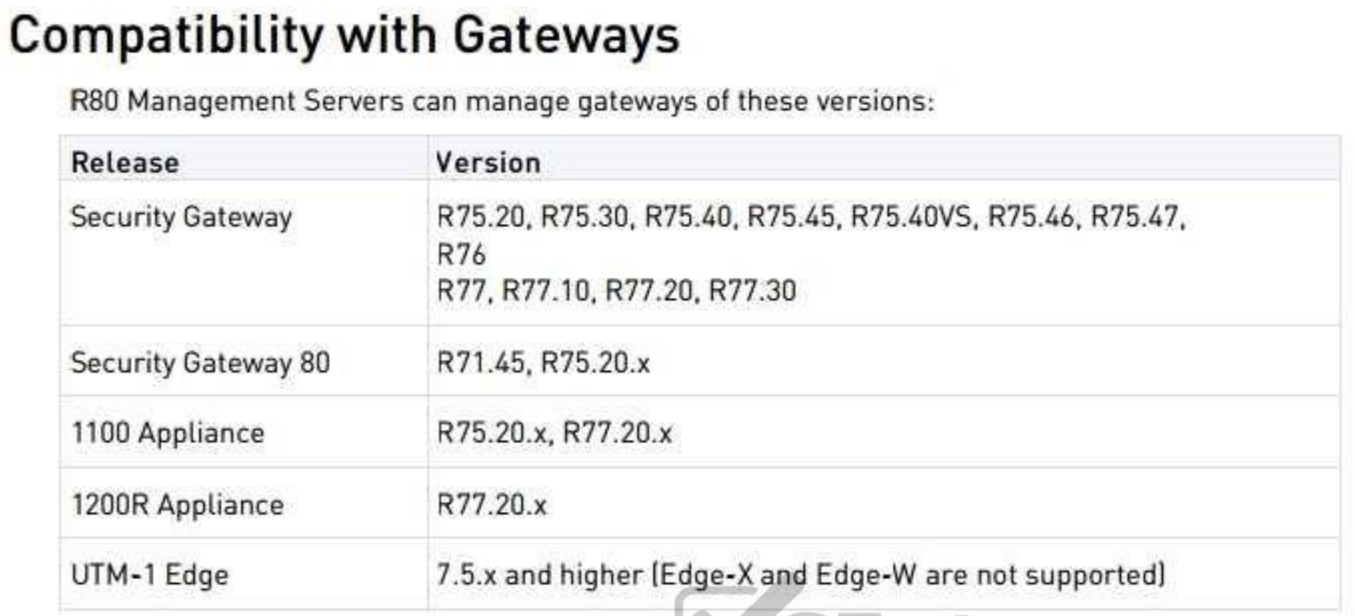
B. R80 Management requires the separate installation of compatibility hotfix packages for managing the earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.

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:



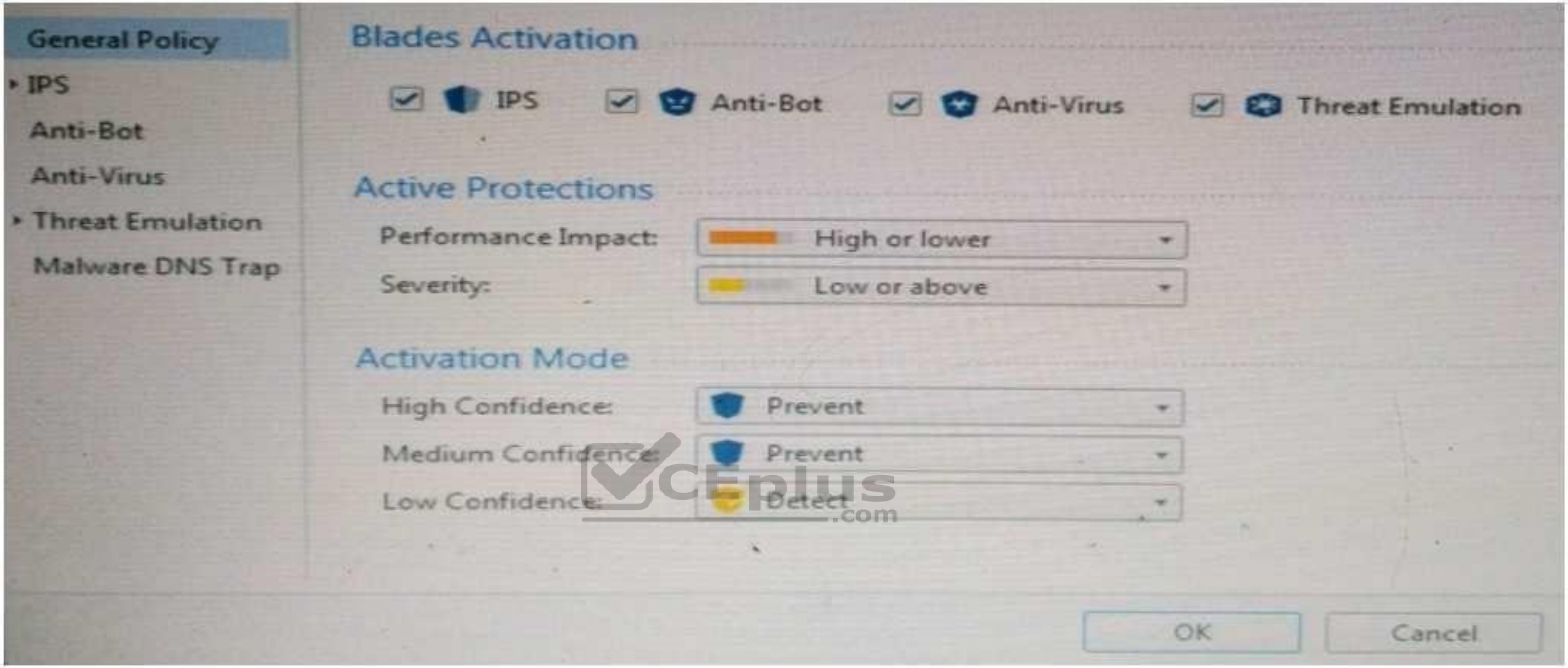
Compatibility with Gateways

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 93
Provide very wide coverage for all products and protocols, with noticeable performance impact.



Blades Activation

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

Active Protections

Performance Impact: High or lower

Severity: Low or above

Activation Mode

High Confidence: Prevent

Medium Confidence: Prevent

Low Confidence: Detect

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

A. Set High Confidence to Low and Low Confidence to Inactive.
B. Set the Performance Impact to Medium or lower.
C. The problem is not with the Threat Prevention 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 94

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 95

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

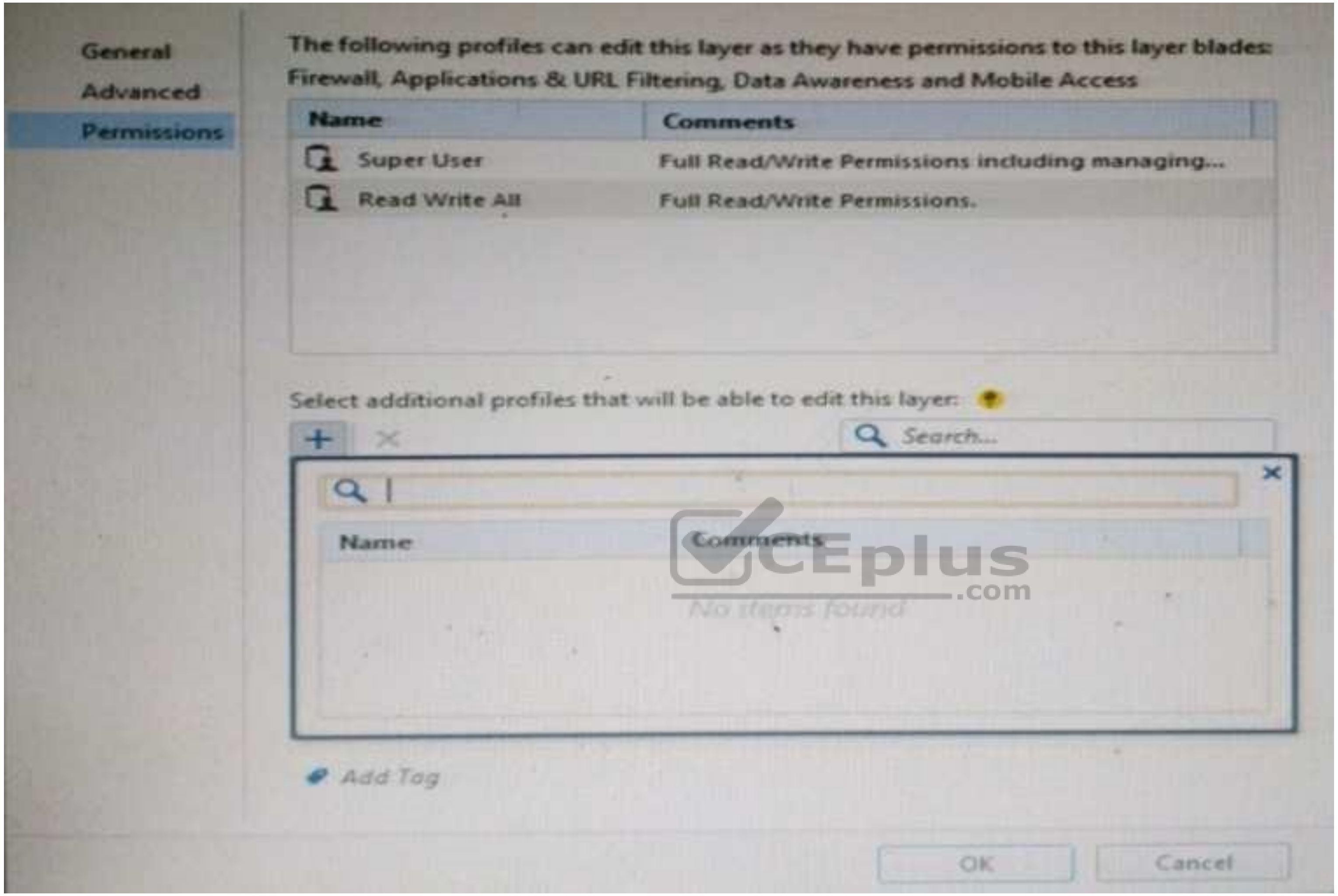
A. Shared policy packages
B. Shared policies
C. Concurrent policy packages
D. Concurrent policies

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96

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



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

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

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

Name	Comments

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

C. All permission profiles are in use.

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
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 98
Fill in the blanks: A High Availability deployment is referred to as a ______ cluster and a Load Sharing deployment is referred to as a ________ cluster.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

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

QUESTION 99
AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule? Choose the BEST answer.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which of the following is TRUE about the Check Point Host object?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: A Check Point host is a host with only one interface, on which Check Point software has been installed, and which is managed by the Security Management server. It is not a routing mechanism and is not capable of IP forwarding.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/13139

QUESTION 101

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

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 102
Which command is used to obtain the configuration lock in Gaia?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: Obtaining a Configuration Lock
▪ `lock database override` ▪ `unlock database`

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

QUESTION 103
Joey is using the computer with IP address 192.168.20.13. He wants to access web page “www.Check Point.com”, which is hosted on Web server with IP address 203.0.113.111. How many rules on Check Point Firewall are required for this connection?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Fill in the blank: Licenses can be added to the License and Contract repository ________ .

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 105
Fill in the blank: A(n) _____ rule is created by an administrator and is located before the first and before last rules in the Rule Base.

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

Correct Answer: E
Section: (none)

Explanation

Explanation/Reference:
Explanation: This is the order that rules are enforced:

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

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

QUESTION 106
Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _______ .

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 107
Fill in the blank: RADIUS Accounting gets ______ data from requests generated by the accounting client

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

Correct Answer: B
Section: (none)

Explanation

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

QUESTION 108
Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and _______ consolidate billions of logs and shows them as prioritized security events.

A. SmartMonitor
B. SmartView Web Application
C. SmartReporter
D. SmartTracker

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: Event Analysis with SmartEvent
The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/131915

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

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

QUESTION 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 Join's desktop which is assigned an IP address 10.0.0.19 via DHCP.

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

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

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

A. John should install the identity Awareness Agent
B. The firewall admin should install the Security Policy
C. John should lock and unlock the computer
D. Investigate this as a network connectivity issue

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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

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 115

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 116
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 117
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 118
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**.

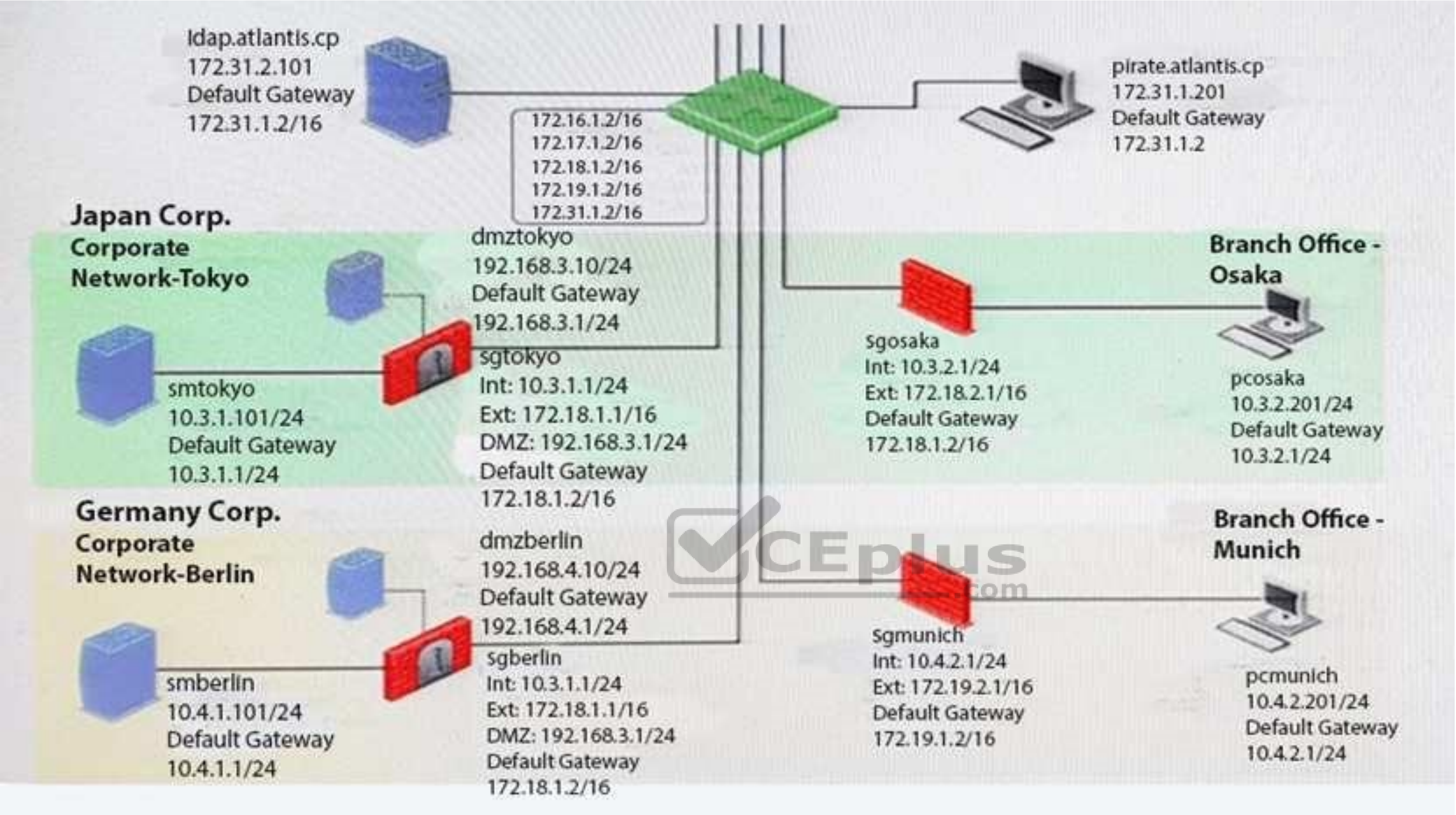
5. Install the Security Policy.

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

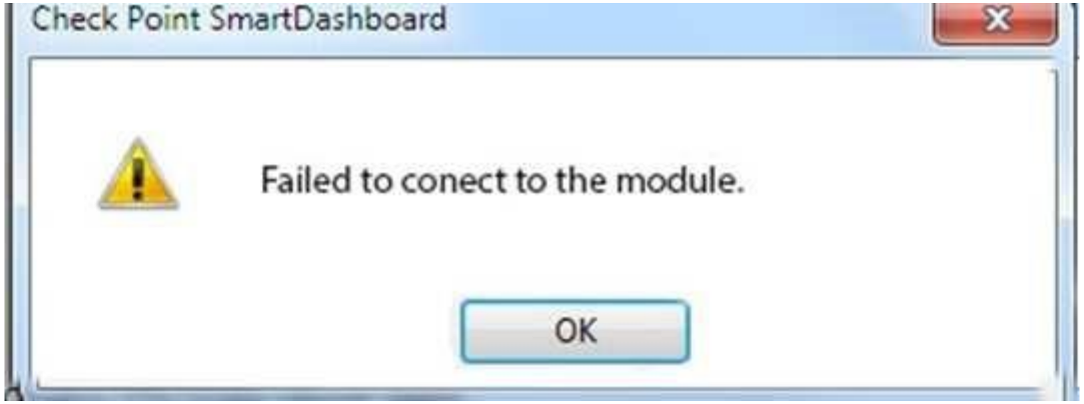
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
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:



Check Point SmartDashboard

Failed to conect to the module.

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 120
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 121

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 122

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 123

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 124
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 125
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 126

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:

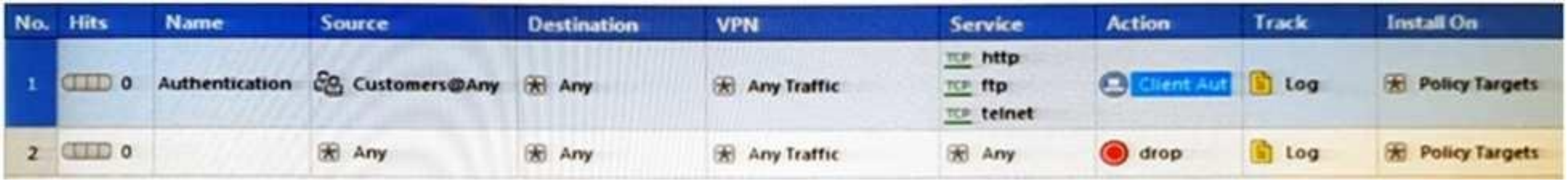
QUESTION 127
You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how many often the particular rules match. Where can you see it? Give the BEST answer.

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.

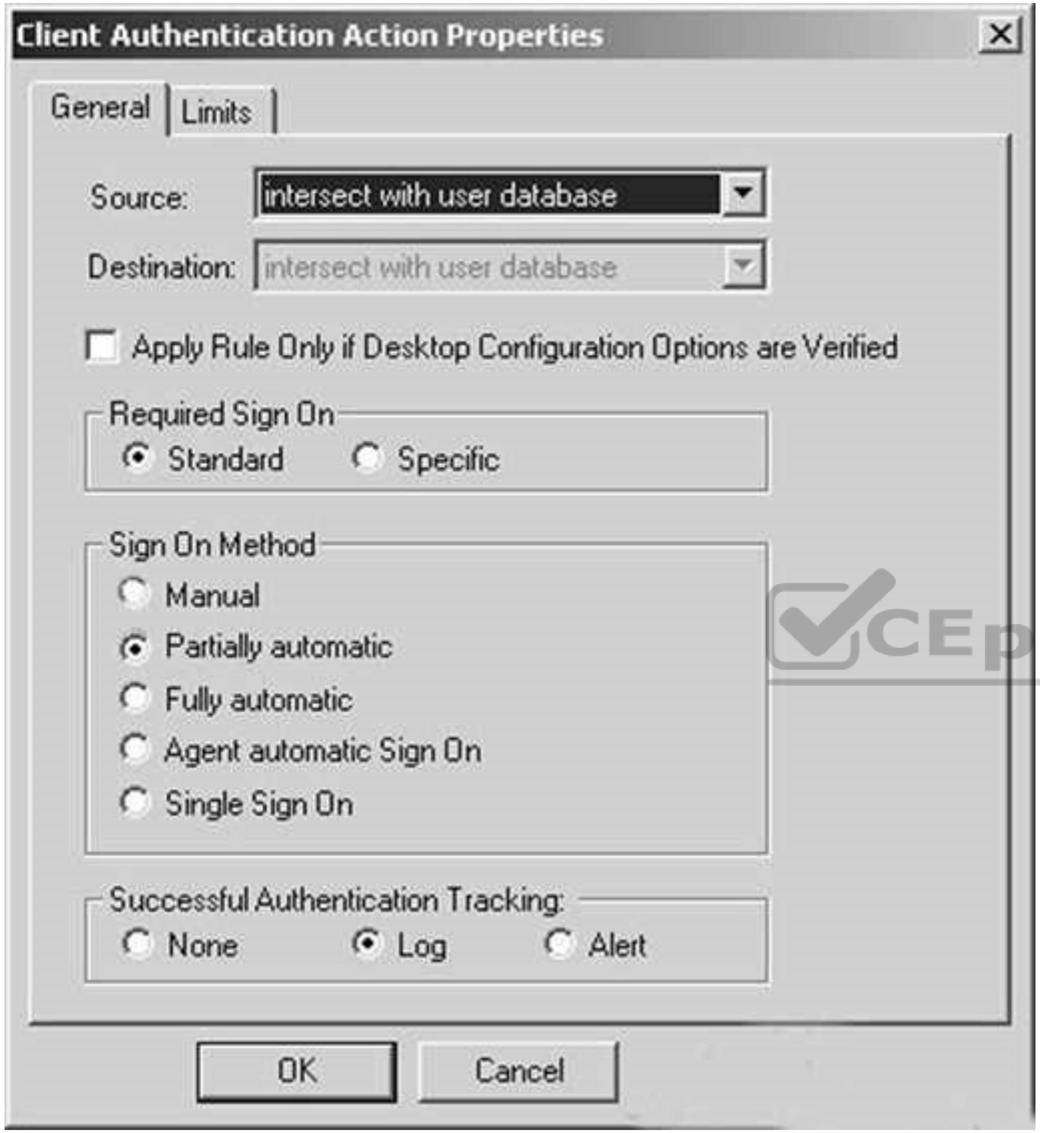
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Study the Rule base and **Client Authentication Action** properties screen.



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



Client Authentication Action Properties

General | Limits

Source: intersect with user database

Destination: intersect with user database

□ Apply Rule Only if Desktop Configuration Options are Verified

Required Sign On
● Standard ○ Specific

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

Successful Authentication Tracking:
○ None ● Log ○ Alert

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
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 130
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 131
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:

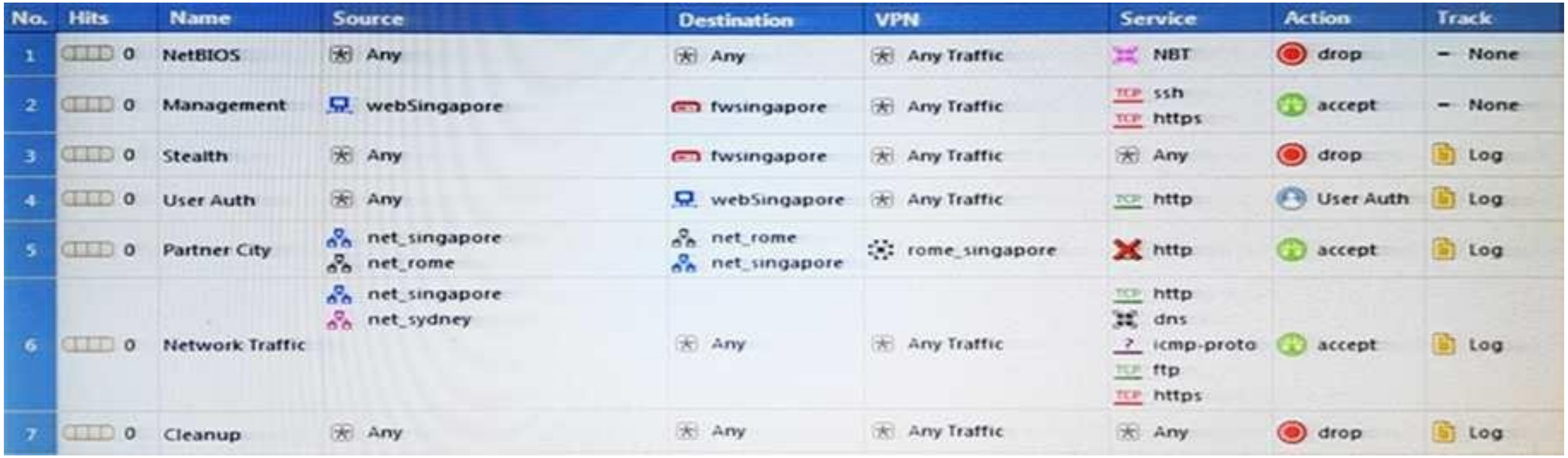
QUESTION 132
Which set of objects have an **Authentication** tab?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
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 134
Which tool CANNOT be launched from SmartUpdate R77?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
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 136
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 137
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 138
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. **Lof 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 139
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 140

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?

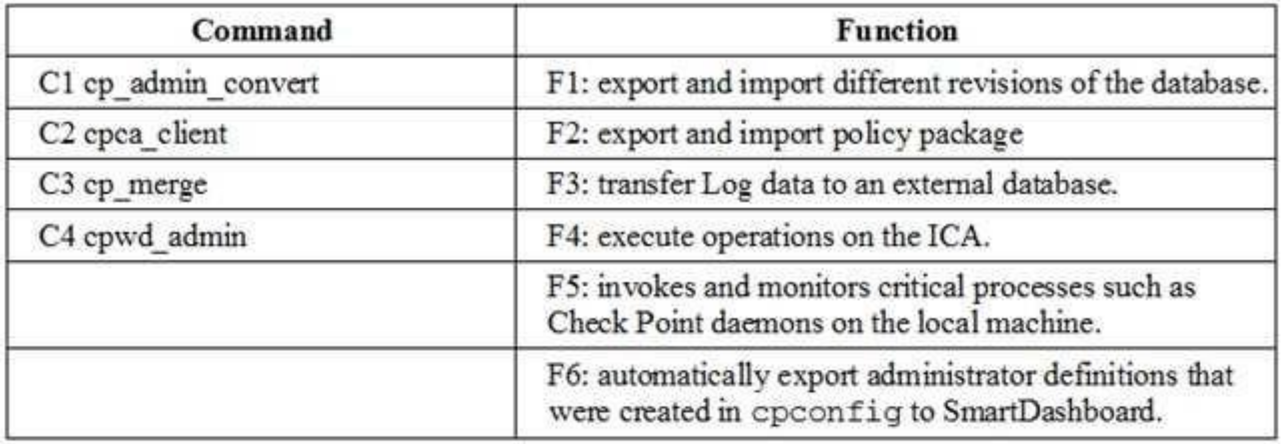
A. Use SmartView Tracker to follow his actions by filtering log entries that feature the WinSCP destination port. Then, export the corresponding entries to a separate log file for documentation.
B. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential 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 141

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 cpca_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 142
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 143
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 144
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 145
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 146
Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
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 148
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 149
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 150
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 151

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 152

What is the Manual Client Authentication TELNET port?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 153

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

To make this scenario work, the IT administrator must:

1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.

3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action. 4) Install policy. Ms McHanry tries to access the resource but is unable. What should she do?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
How many packets does the IKE exchange use for Phase 1 Main Mode?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 155
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 156
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:

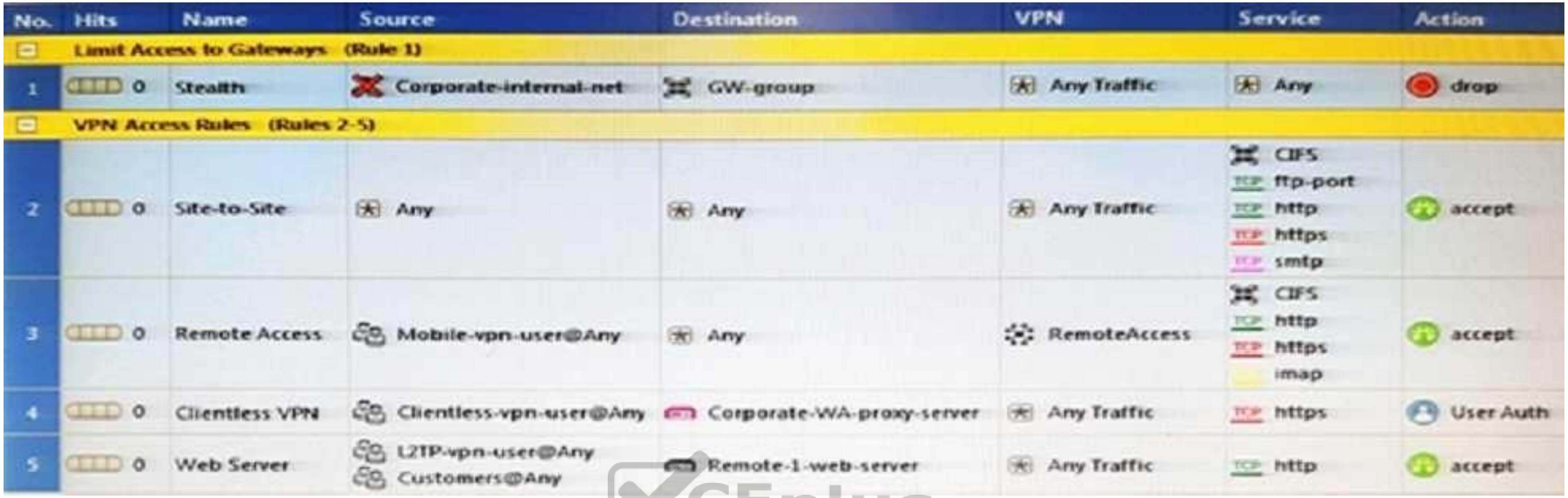
QUESTION 157
Which of the following is NOT a valid option when configuring access for Captive Portal?

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 158
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 159

What happens when you run the command: `fw sam -J src [Source IP Address]`?

A. Connections from the specified source are blocked without the need to change the Security Policy.

B. Connections to the specified target are blocked without the need to change the Security Policy.

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

D. Connections to and from the specified target are blocked with the need to change the Security Policy.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
VPN gateways must authenticate to each other prior to exchanging information. What are the two types of credentials used for authentication?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added? A (n):

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
You are about to integrate RSA SecurID users into the Check Point infrastructure. What kind of users are to be defined via SmartDashboard?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Where does the security administrator activate Identity Awareness within SmartDashboard?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.
John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his desktop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.
To make this scenario work, the IT administrator:
1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location. 3) Changes from static IP address to DHCP for the client PC.
What should John request when he cannot access the web server from his laptop?

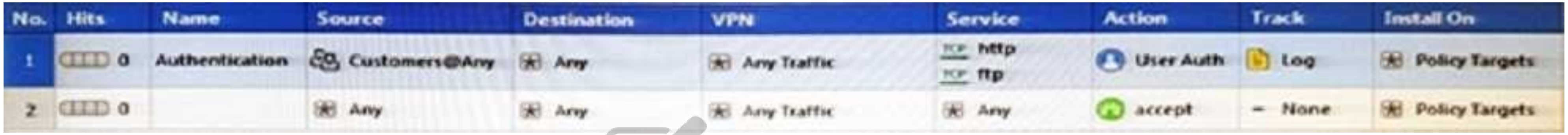
A. John should lock and unlock his computer

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
Review the rules. Assume domain UDP is enabled in the implied rules.



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

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:
A. can connect to the Internet successfully after being authenticated.
B. is prompted three times before connecting to the Internet successfully.
C. can go to the Internet after Telnetting to the client authentication daemon port 259.
D. can go to the Internet, without being prompted for authentication.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Which component functions as the Internal Certificate Authority for R77?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
Check Point APIs allow system engineers and developers to make changes to their organization's security policy with CLI tools and Web Services for all of the following except:

A. Create new dashboards to manage 3rd party task
B. Create products that use and enhance 3rd party solutions
C. Execute automated scripts to perform common tasks
D. Create products that use and enhance the Check Point Solution

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf?HashKey=1517081623_70199443034f806cf2dd0a7ba15f201c&xtn=.pdf

QUESTION 170
In what way are SSL VPN and IPSec VPN different?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
Which command can you use to enable or disable multi-queue per interface?

A. cpmq set
B. Cpmqueue set
C. Cpmq config
D. Set cpmq enable

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/93689.htm

QUESTION 172
Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?
A. There is no traffic queue to be handled
B. Several NICs can use one traffic queue by one CPU
C. Each NIC has several traffic queues that are handled by multiple CPU cores
D. Each NIC has one traffic queue that is handled by one CPU

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/93689.htm

QUESTION 173
To fully enable Dynamic Dispatcher on a Security Gateway:

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk105261#Configuration%20R80.10

QUESTION 174
What are types of Check Point APIs available currently as part of R80.10 code?

A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API
B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
C. OSE API, OPSEC SDK API, Threat Prevention API and Policy Editor API
D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf?HashKey=1517088487_4c0acda205460a92f44c83d399826a7b&xtn=.pdf

QUESTION 175
What is the purpose of Priority Delta in VRRP?

A. When a box is up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fails, Effective Priority = Priority - Priority Delta
D. When a box fails, Effective Priority = Priority - Priority Delta

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 176
The Firewall kernel is replicated multiple times, therefore:

A. The Firewall kernel only touches the packet if the connection is accelerated
B. The Firewall can run different policies per core
C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
D. The Firewall can run the same policy on all cores

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 177
There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?

A. Using Web Services
B. Using Mgmt_cli tool
C. Using CLISH
D. Using SmartConsole GUI console

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf?HashKey=1517088487_4c0acda205460a92f44c83d399826a7b&xtn=.pdf

QUESTION 178
Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Mobile_Access_WebAdmin/41587.htm

QUESTION 179
Which command can you use to verify the number of active concurrent connections?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk103496

QUESTION 180
Which remote Access Solution is clientless?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/92708.htm

QUESTION 181
What component of R80 Management is used for indexing?

A. DBSync
B. API Server
C. fwm
D. SOLR

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/downloads/product-related/r80.10-mgmt-architecture-overview.pdf

QUESTION 182
Which NAT rules are prioritized first?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
What is the difference between an event and a log?

A. Events are generated at gateway according to Event Policy
B. A log entry becomes an event when it matches any rule defined in Event Policy
C. Events are collected with SmartWorkflow from Trouble Ticket systems

D. Logs and Events are synonyms

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186
Which one of the following is true about Threat Extraction?

A. Always delivers a file to user
B. Works on all MS Office, Executables, and PDF files
C. Can take up to 3 minutes to complete
D. Delivers file only if no threats found

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
Which is the correct order of a log flow processed by SmartEvent components:
A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
Which of these statements describes the Check Point ThreatCloud?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.checkpoint.com/support-services/threatcloud-managed-security-service/

QUESTION 189
Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 190
When defining QoS global properties, which option below is not valid?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 191
The WebUI offers three methods for downloading Hotfixes via CPUSE. One of them is Automatic method. How many times per day will CPUSE agent check for hotfixes and automatically download them?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 192
What is the benefit of Manual NAT over Automatic NAT?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 193
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 194

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 195

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 196

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

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

D. mgmt add host name emailserver1 ip-address 10.50.23.90

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
The CDT utility supports which of the following?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 198
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 199
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 200
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 201
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 202
What are the three components for Check Point Capsule?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 203
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 204
What is true about the IPS-Blade?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 205
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 206
When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

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 207
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 208
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 209
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 210
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 211
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 212
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 213
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 214
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 215
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 216
Which of the following is NOT an option to calculate the traffic direction?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 217
When an encrypted packet is decrypted, where does this happen?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 218
Which of the following is NOT a component of Check Point Capsule?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 219
You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

A. restore_backup

B. import backup
C. cp_merge
D. migrate import

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 220
What is the best sync method in the ClusterXL deployment?

A. Use 1 cluster + 1st sync
B. Use 1 dedicated sync interface
C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
D. Use 2 clusters + 1st sync + 2nd sync

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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?

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
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 237
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 238
Which of the following is an authentication method used for Identity Awareness?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 239

The SIC Status “Unknown” means

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SIC Status
After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:
Communicating - The secure communication is established.
Unknown - There is no connection between the gateway and Security Management Server.
Not Communicating - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/125443

QUESTION 240
What is a reason for manual creation of a NAT rule?

A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.
C. Network Address Translation is desired for some services, but not for others.
D. The public IP-address is different from the gateway’s external IP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 241
Which of the following commands is used to verify license installation?

A. Cplic verify license

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242
To enforce the Security Policy correctly, a Security Gateway requires:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:
Correctly enforce the Security Policy.
Ensure the validity of IP addresses for inbound and outbound traffic.
Configure a special domain for Virtual Private Networks.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/118037

QUESTION 243
Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

A. The firewall topologies
B. NAT Rules
C. The Rule Base

D. The VPN Domains

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

QUESTION 244
Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 245
Which GUI tool can be used to view and apply Check Point licenses?

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

Correct Answer: D
Section: (none)
Explanation

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

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/79993

QUESTION 246

In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

A. 3rd Party integration of CLI and API for Gateways prior to R80.
B. A complete CLI and API interface using SSH and custom CPCode integration.
C. 3rd Party integration of CLI and API for Management prior to R80.
D. A complete CLI and API interface for Management with 3rd Party integration.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 247

When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 248

Fill in the blank: To create policy for traffic to or from a particular location, use the _____________.

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

D. HTTPS inspection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Shared Policies
The **Shared Policies** section in the **Security Policies** shows the policies that are not in a Policy package. They are shared between all Policy packages. Shared policies are installed with the Access Control Policy.

Software Blade	Description
Mobile Access	Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP	Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy	Create a policy for traffic to or from specific geographical or political locations.

Reference: https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_NexGenSecurityGateway_Guide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_NexGenSecurityGateway_Guide/137006

QUESTION 249
After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

A. Security Gateway IP-address cannot be changed without re-establishing the trust
B. The Security Gateway name cannot be changed in command line without re-establishing trust
C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 250

Which two Identity Awareness commands are used to support identity sharing?

A. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
C. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
D. Policy Activation Point (PAP) and Policy Decision Point (PDP)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/66477.htm

QUESTION 251
Which one of the following is TRUE?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 252
Fill in the blank: An identity server uses a ___________ for user authentication.

A. Shared secret
B. Certificate
C. One-time password
D. Token

Correct Answer: A
Section: (none)
Explanation

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