156-215.80.288q

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

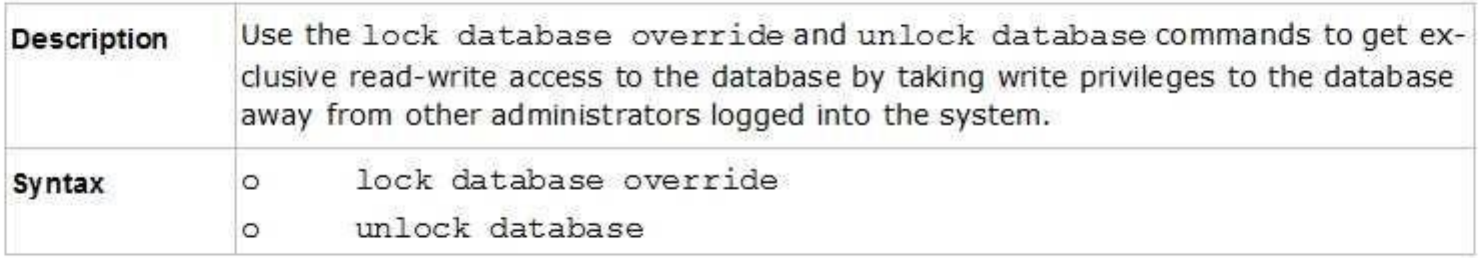
Correct Answer: B
Section: (none)
Explanation

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.

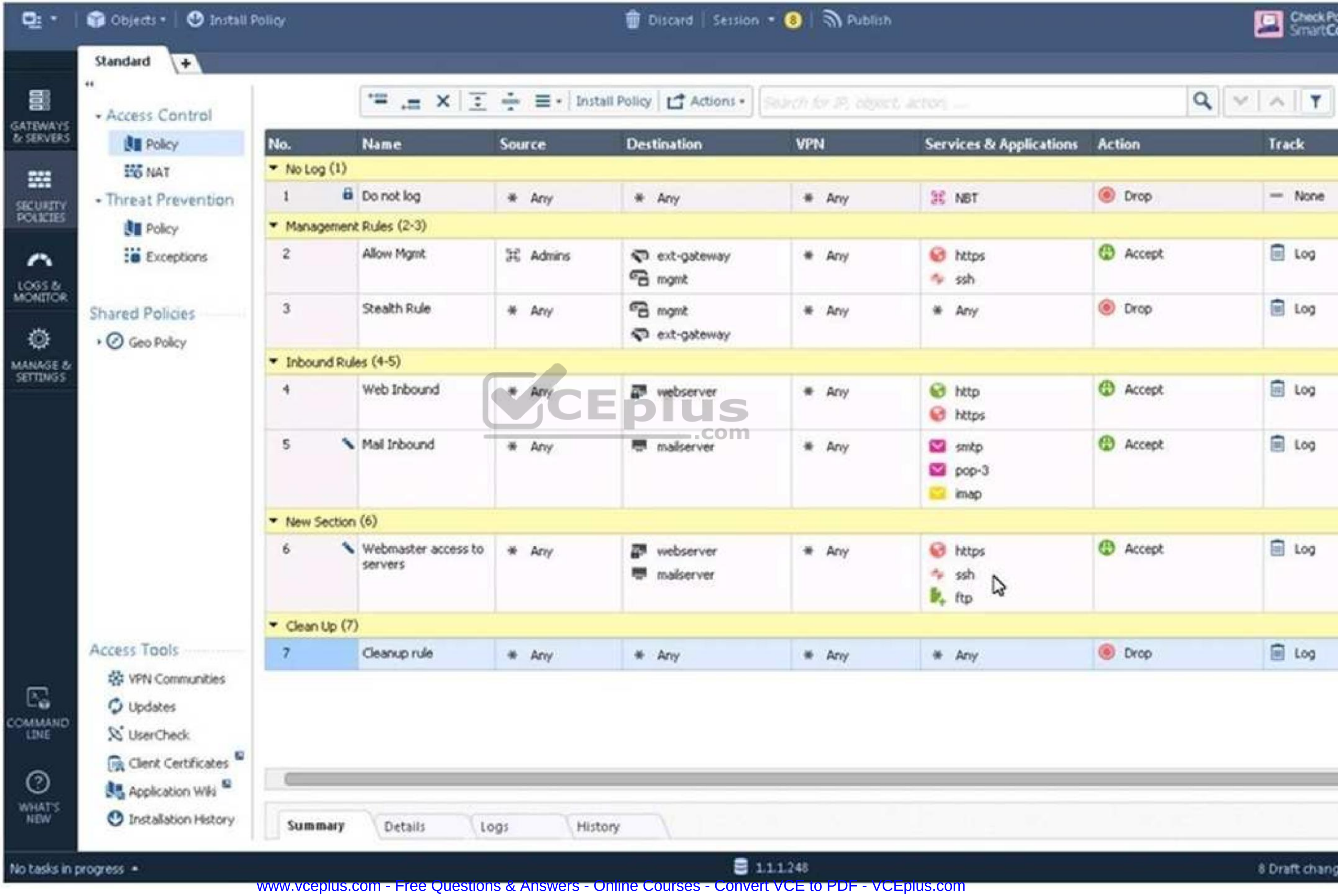
Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Use the *database* feature to obtain the configuration lock. The database feature has two commands:
`▪ lock database [override]. ▪ unlock database`
The commands do the same thing: obtain the configuration lock from another 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.



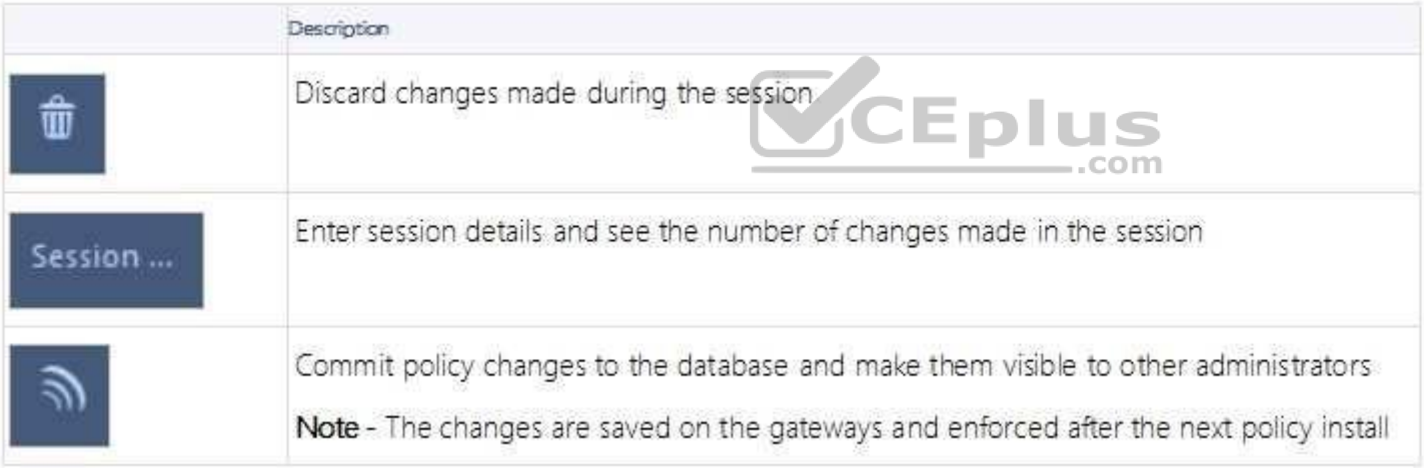
No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	Any	Any	Any	NBT	Drop	None
Management Rules (2-3)							
2	Allow Mgmt	Admins	ext-gateway mgmt	Any	https ssh	Accept	Log
3	Stealth Rule	Any	mgmt ext-gateway	Any	Any	Drop	Log
Inbound Rules (4-5)							
4	Web Inbound	Any	webserver	Any	http https	Accept	Log
5	Mail Inbound	Any	mailserver	Any	smtp pop-3 imap	Accept	Log
New Section (6)							
6	Webmaster access to servers	Any	webserver mailserver	Any	https ssh ftp	Accept	Log
Clean Up (7)							
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

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)

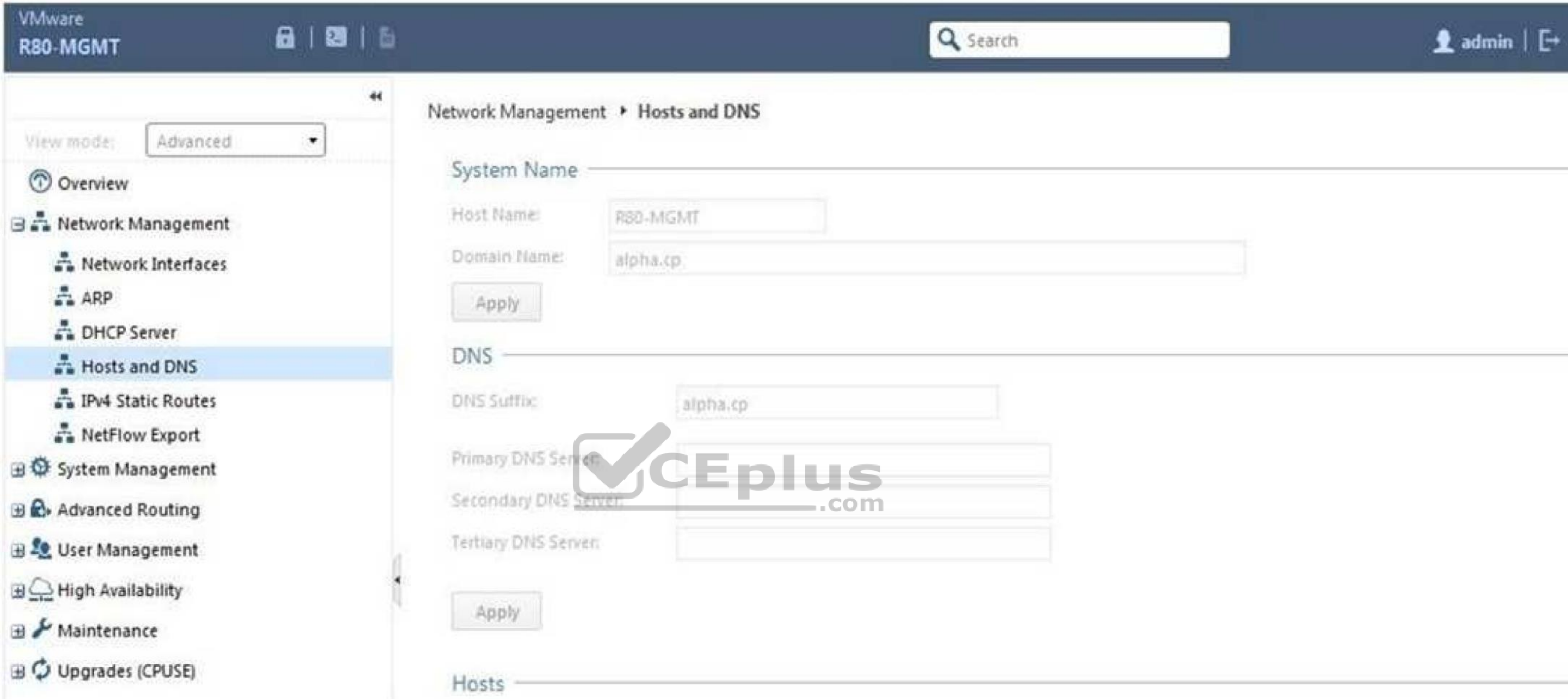


	Description
🗑	Discard changes made during the session
Session ...	Enter session details and see the number of changes made in the session
	Commit policy changes to the database and make them visible to other administrators **Note** - The changes are saved on the gateways and enforced after the next policy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

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

QUESTION 10
ALPHA Corp has a new administrator who logs into the Gaia Portal to make some changes. He realizes that even though he has logged in as an administrator, he is unable to make any changes because all configuration options are greyed out as shown in the screenshot image below. What is the likely cause for this?

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



VMware
R80-MGMT

Search

admin

View mode: Advanced

- Overview
- Network Management
  - Network Interfaces
  - ARP
  - DHCP Server
  - Hosts and DNS
  - IPv4 Static Routes
  - NetFlow Export
- System Management
- Advanced Routing
- User Management
- High Availability
- Maintenance
- Upgrades (CPUSE)

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

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

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 12

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 13

By default, which port does the WebUI listen on?

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

Correct Answer: C
Section: (none)
Explanation

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

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

QUESTION 14
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 15

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 16
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.

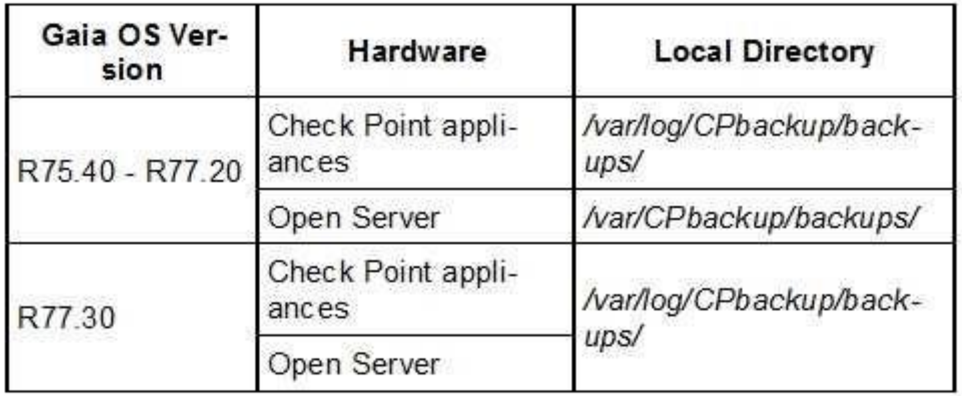
Reference: http://dl3.checkpoint.com/paid/74/74d596decb6071a4ee642fbdaae7238f/CP_R80_SecurityManagement_AdminGuide.pdf?HashKey=1479584563_6f823c8ea1514609148aa4fec5425db2&xtn=.pdf

QUESTION 17
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 18
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 19
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 20

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 21

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 22

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 23
Fill in the blank: A new license should be generated and installed in all of the following situations **EXCEPT** when ________ .

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 24
What is the default shell for the command line interface?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 25
When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SmartUpdate installs two *repositories* on the Security Management server:
▪ **License & Contract Repository**, which is stored on all platforms in the directory `$FWDIR\conf\`. ▪
Package Repository, which is stored:

- on Windows machines in `C:\SUroot`.
- on UNIX machines in `/var/suroot`.

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

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

QUESTION 26
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 27
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 28
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 29
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?

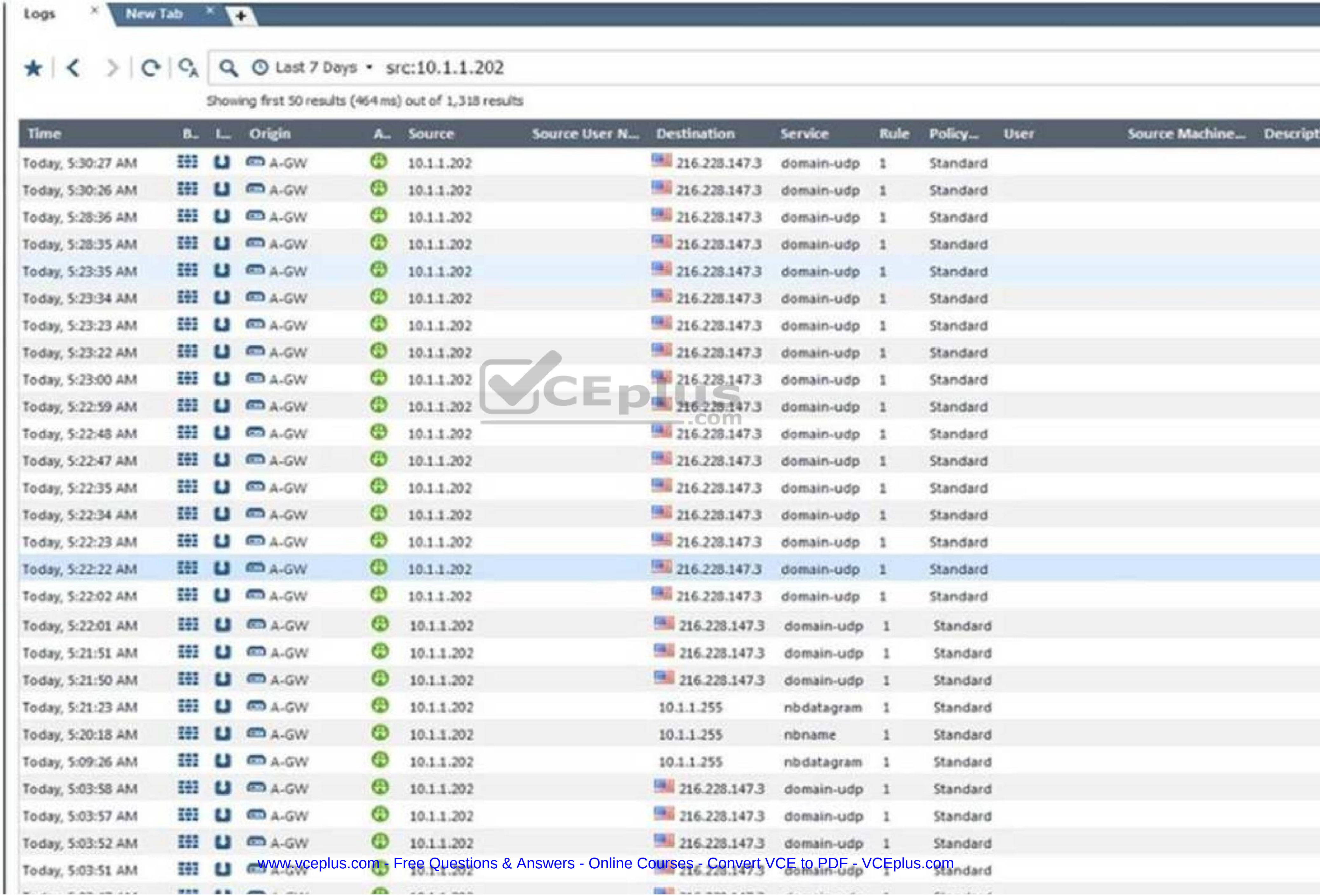
A. `cpconfig`
B. `fw ctl pstat`
C. `cpview`
D. `fw ctl multik stat`

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 30
The following graphic shows:



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...	Descript
Today, 5:30:27 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:30:26 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:36 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:28:35 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:35 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:34 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:23 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:22 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:23:00 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:59 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:48 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:47 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:35 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:34 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:23 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:22 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:02 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:22:01 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:51 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:50 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:21:23 AM			A-GW		10.1.1.202		10.1.1.255	nbdatagram	1	Standard			
Today, 5:20:18 AM			A-GW		10.1.1.202		10.1.1.255	nbname	1	Standard			
Today, 5:09:26 AM			A-GW		10.1.1.202		10.1.1.255	nbdatagram	1	Standard			
Today, 5:03:58 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:57 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:52 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			
Today, 5:03:51 AM			A-GW		10.1.1.202		216.228.147.3	domain-udp	1	Standard			

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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 32
Fill in the blank: The command __________ provides the most complete restoration of a R80 configuration.

A. `upgrade_import`

B. `cpconfig`

C. `fwm dbimport -p <export file>`

D. `cpinfo -recover`

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 33
The Gaia operating system supports which routing protocols?

A. BGP, OSPF, RIP

B. BGP, OSPF, EIGRP, PIM, IGMP

C. BGP, OSPF, RIP, PIM, IGMP

D. BGP, OSPF, RIP, EIGRP

Correct Answer: A
Section: (none)
Explanation

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

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

QUESTION 34
Joey wants to configure NTP on R80 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

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

Correct Answer: A
Section: (none)
Explanation

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

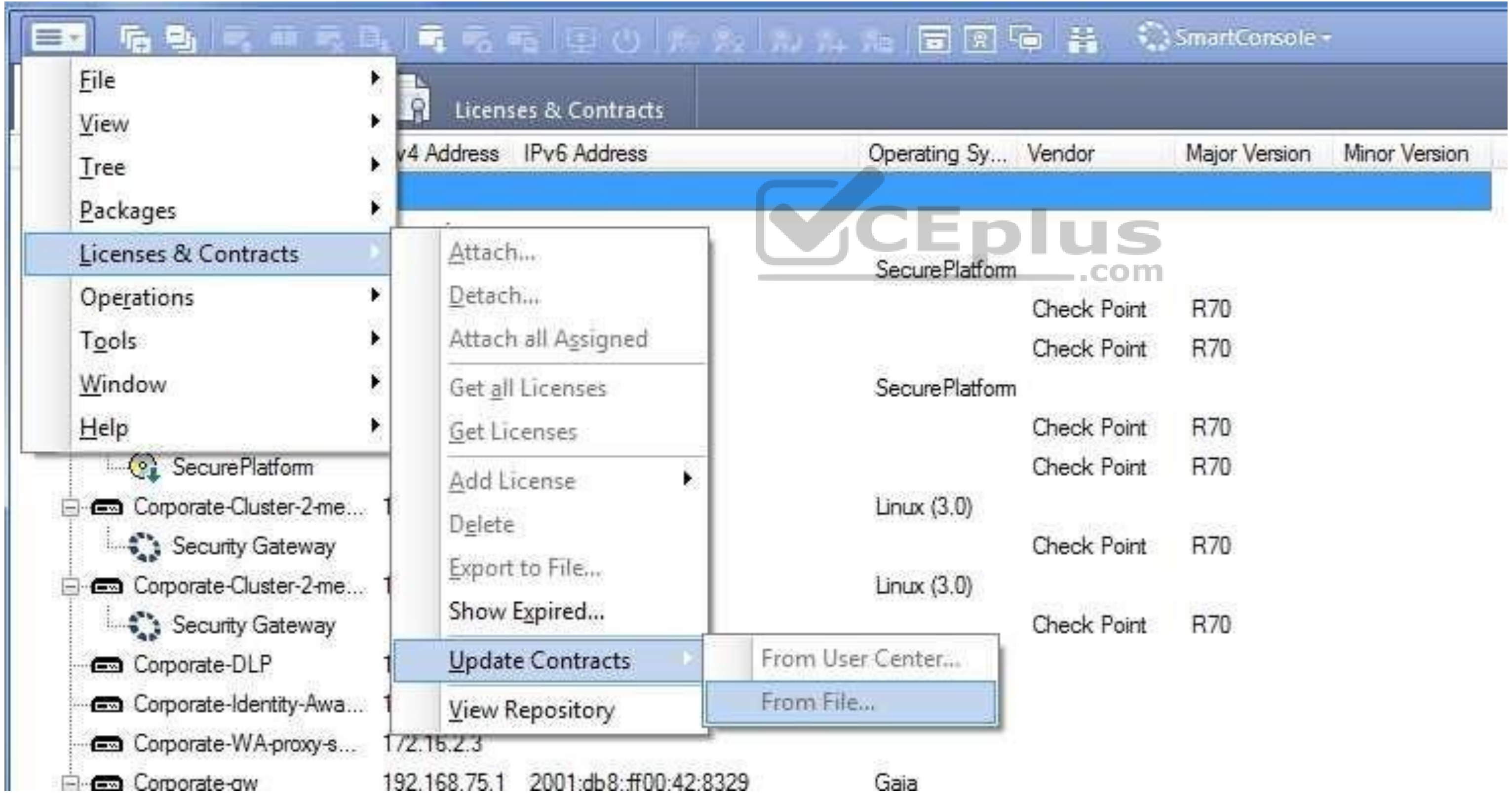
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/75930

QUESTION 35
Which application should you use to install a contract file?

A. SmartView Monitor
B. WebUI

C. SmartUpdate
D. SmartProvisioning

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 / Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.
Open SmartUpdate and from the Launch Menu select '`Licenses & Contracts`' -> '`Update Contracts`' -> '`From File...`' and provide the path to the file you have downloaded in Step #3:



Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk33089

QUESTION 36
Which feature is NOT provided by all Check Point Mobile Access solutions?

A. Support for IPv6
B. Granular access control
C. Strong user authentication
D. Secure connectivity

Correct Answer: A
Section: (none)
Explanation

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

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

QUESTION 37
You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

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

Correct Answer: D

Section: (none)
Explanation

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

QUESTION 38
Fill in the blank: Each cluster has __________ interfaces.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each cluster member has three interfaces: one external interface, one internal interface, and one for synchronization. Cluster member interfaces facing in each direction are connected via a switch, router, or VLAN switch.

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

QUESTION 39
What are the three essential components of the Check Point Security Management Architecture?

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

Correct Answer: A

Section: (none)
Explanation

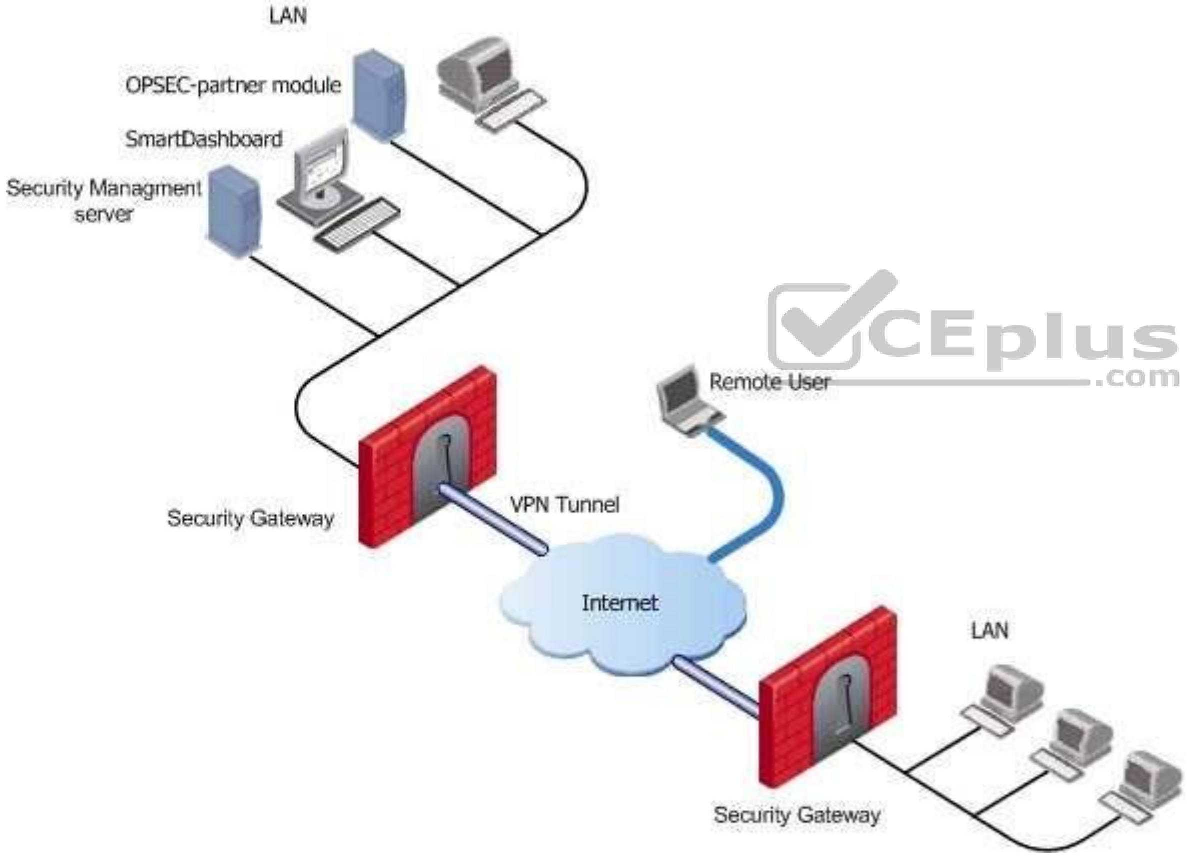
Explanation/Reference:

Explanation:

Deployments

Basic deployments:

- Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.
- Distributed deployment - Security Gateway and the Security Management server are installed on different machines.



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

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

QUESTION 40
What are the two types of address translation rules?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
NAT Rule Base
The NAT Rule Base has two sections that specify how the IP addresses are translated:

- **Original Packet**
- **Translated Packet**

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

QUESTION 41

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

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

A. CDP is down

B. SVR is down

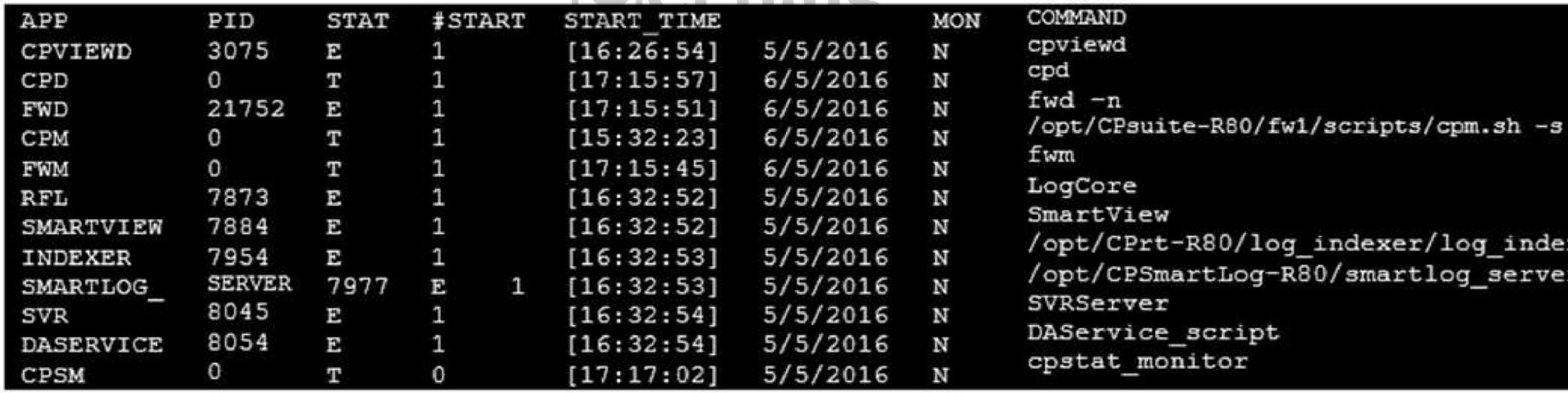
C. FWM is down

D. CPSM is down

Correct Answer: C
Section: (none)
Explanation

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

- SmartDashboard fails to connect to the Security Management server.



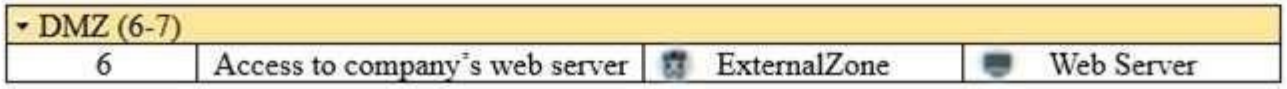
```
APP          PID     STAT  #START  START_TIME                  MON  COMMAND
CPVIEWD      3075    E     1       [16:26:54]  5/5/2016        N    cpviewd
CPD          0       T     1       [17:15:57]  6/5/2016        N    cpd
FWD          21752   E     1       [17:15:51]  6/5/2016        N    fwd -n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

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

[Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"

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

QUESTION 42
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 43

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 44

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 45
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 46
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 47

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 48

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.

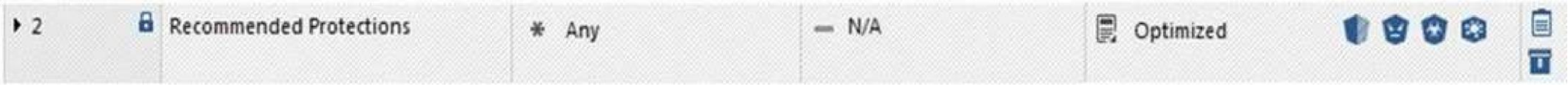
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62050.htm

QUESTION 49
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:



2 Recommended Protections | Any | N/A | Optimized

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 50
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 51
Which command is used to add users to or from existing roles?

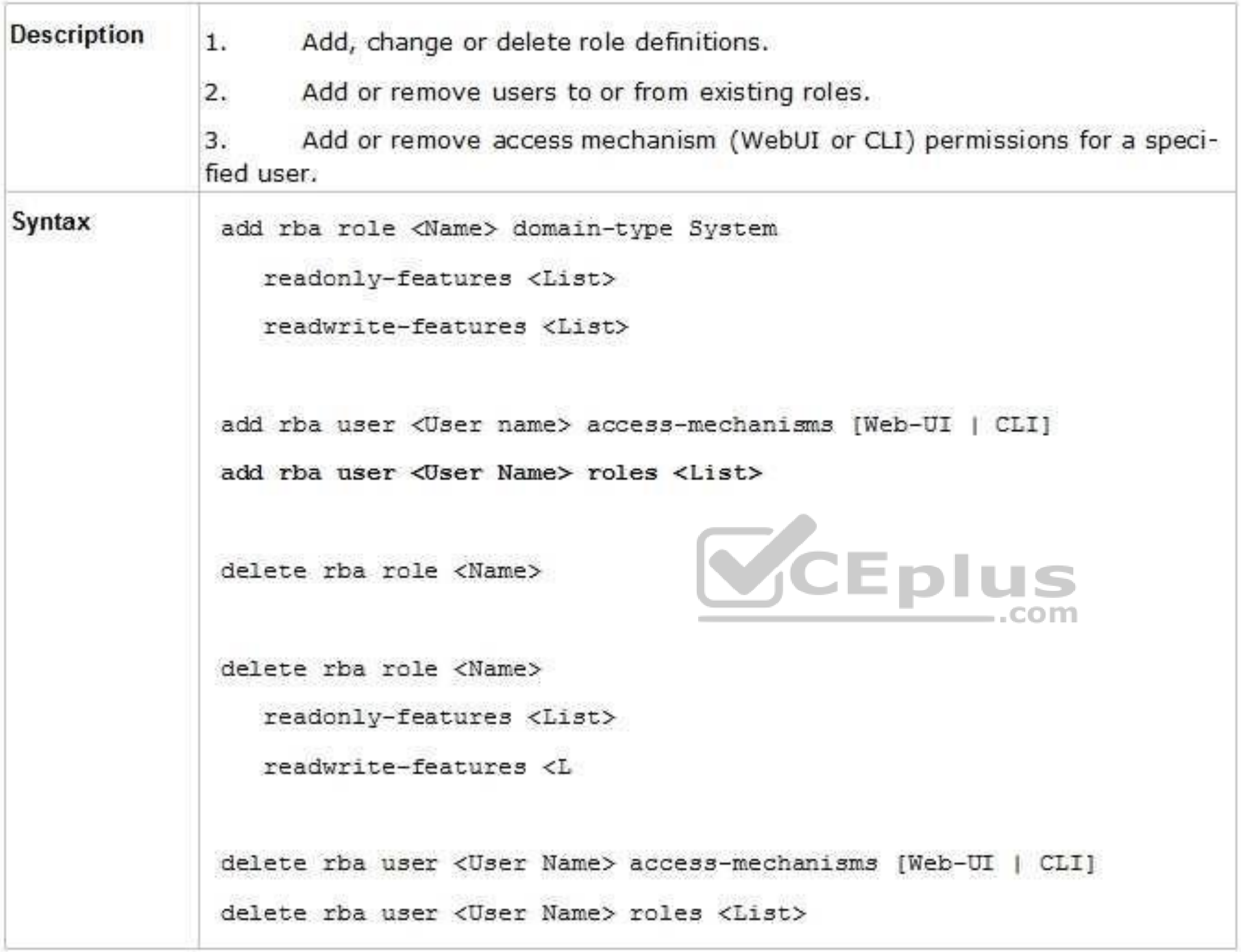
A. Add rba user <User Name> roles <List>
B. Add rba user <User Name>
C. Add user <User Name> roles <List>
D. Add user <User Name>

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Configuring Roles - CLI (rba)



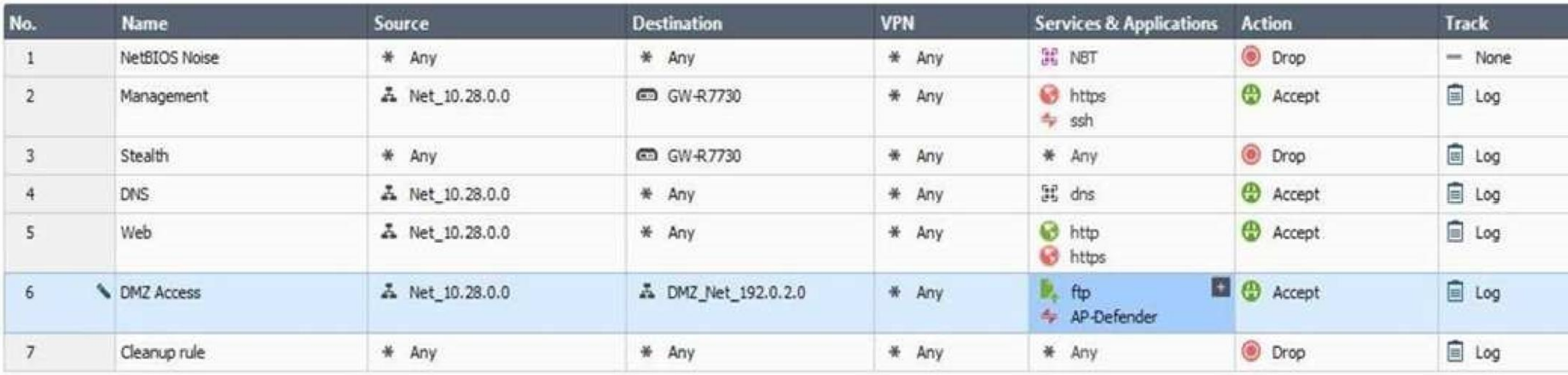
Description	1. Add, change or delete role definitions. 2. Add or remove users to or from existing roles. 3. Add or remove access mechanism (WebUI or CLI) permissions for a specified user.

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 52

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



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	NetBIOS Noise	Any	Any	Any	NBT	Drop	None
2	Management	Net_10.28.0.0	GW-R7730	Any	https ssh	Accept	Log
3	Stealth	Any	GW-R7730	Any	Any	Drop	Log
4	DNS	Net_10.28.0.0	Any	Any	dns	Accept	Log
5	Web	Net_10.28.0.0	Any	Any	http https	Accept	Log
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	Any	ftp AP-Defender	Accept	Log
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

What does this mean?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
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

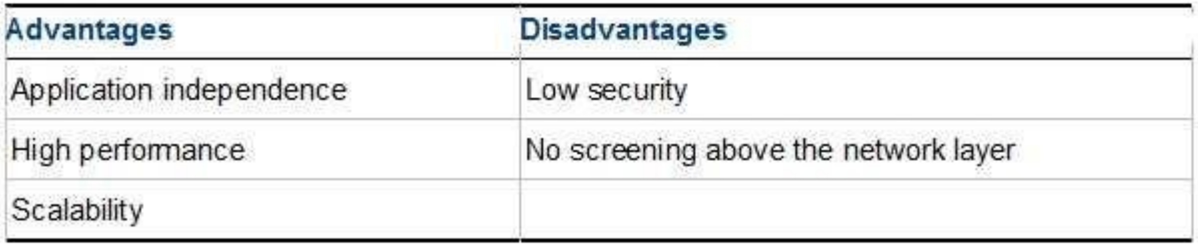
Explanation/Reference:

QUESTION 54
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 55
In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

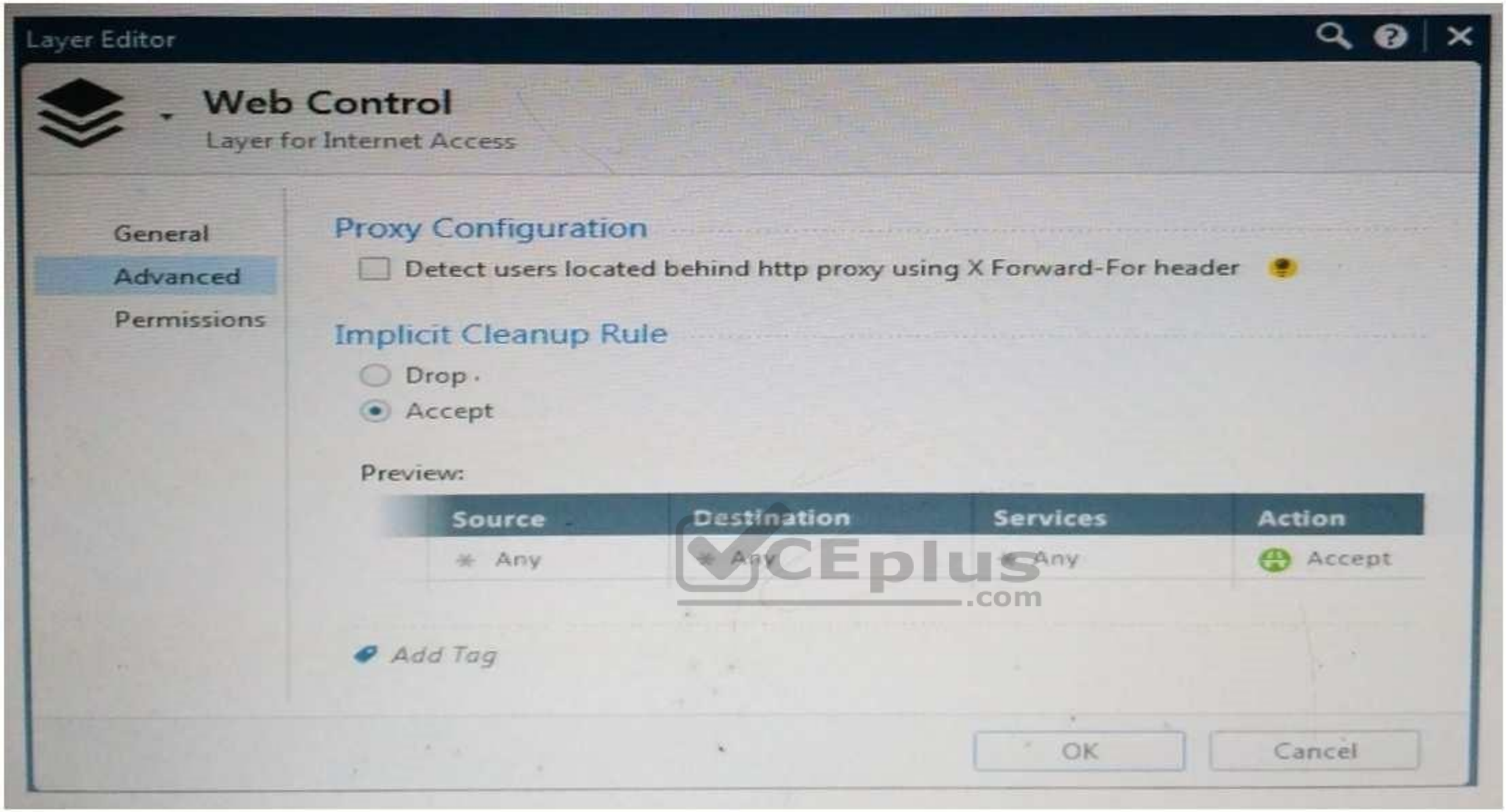
A. Display policies and logs on the administrator's workstation.
B. Verify and compile Security Policies.
C. Processing and sending alerts such as SNMP traps and email notifications.

D. Store firewall logs to hard drive storage.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Web Control Layer has been set up using the settings in the following dialogue:



Layer Editor

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

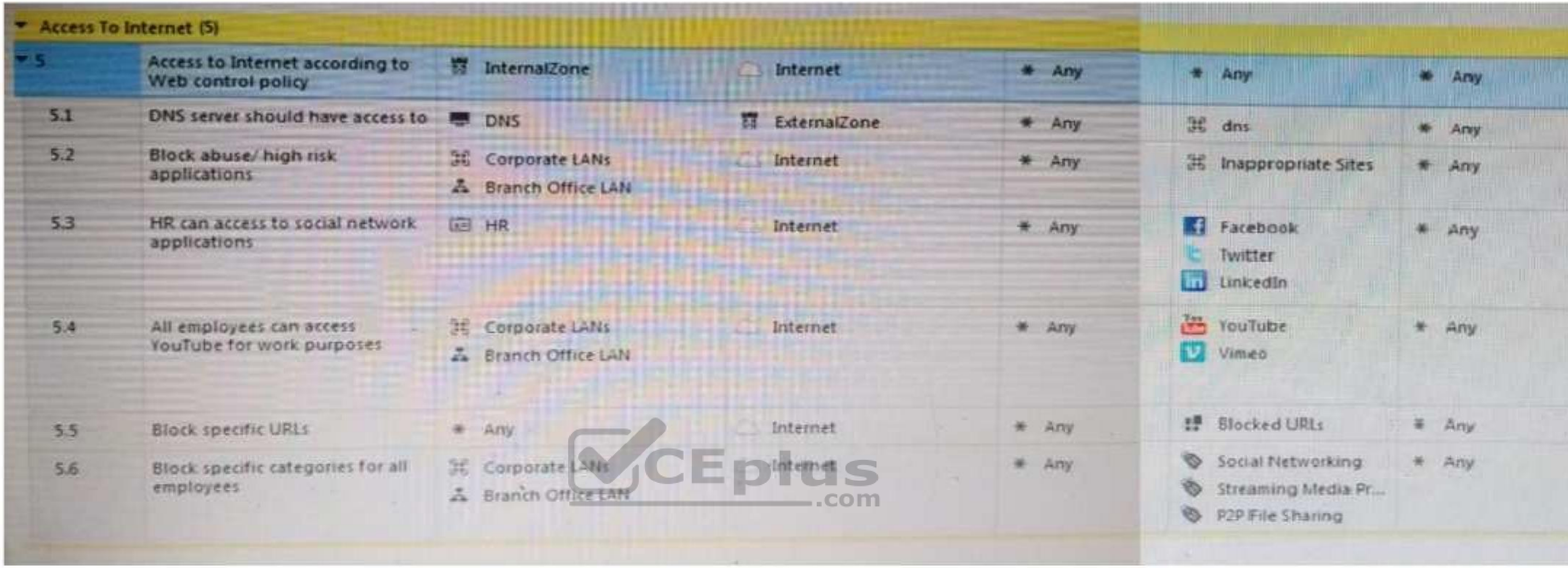
Consider the following policy and select the BEST answer.

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.



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

Correct Answer: D
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 57
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

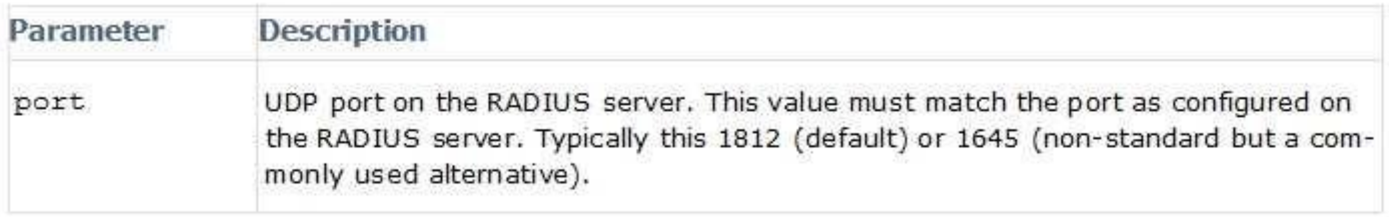
Explanation/Reference:

QUESTION 58
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 59

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 60

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 61
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 62

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

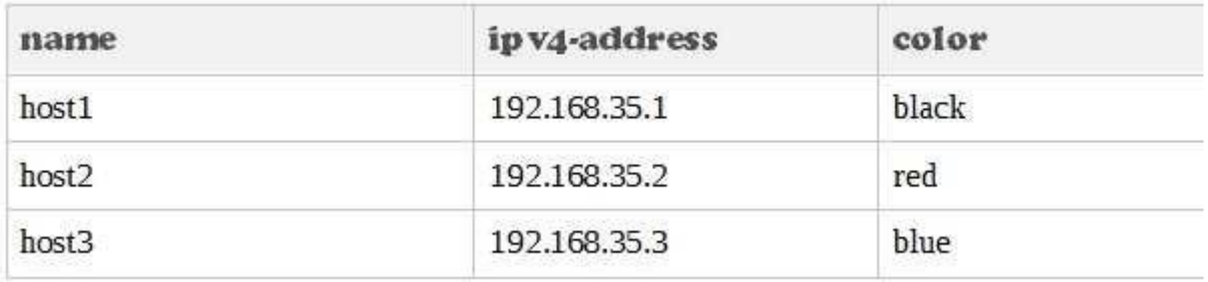
A. Create a text-file with `mgmt_cli` script that creates all objects and policies. Open the file in SmartConsole Command Line to run it.
B. Create a text-file with Gaia CLI -commands in order to create all objects and policies. Run the file in CLISH with command `load configuration`.
C. Create a text-file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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Did you know: mgmt_cli can accept csv files as inputs using the --batch option.
The first row should contain the argument names and the rows below it should hold the values for these parameters.

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

data.csv:



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

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

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

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

QUESTION 63
When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Identity Awareness gets identities from these acquisition sources:
- AD Query
- Browser-Based Authentication
- Endpoint Identity Agent
- Terminal Servers Identity Agent
- Remote Access Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62007.htm

QUESTION 64
Which of the following is NOT a back up method?

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

Correct Answer: A
Section: (none)
Explanation

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

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

QUESTION 65
Which of the following is NOT an advantage to using multiple LDAP servers?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 67
What is the default method for destination NAT?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Client Side NAT - destination is NAT`d by the inbound kernel

QUESTION 68
Choose what BEST describes a Session.

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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
Administrator Collaboration
More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.
When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.
To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/117948

QUESTION 69
Which of the following is **NOT** a VPN routing option available in a star community?

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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SmartConsole
For simple hubs and spokes (or if there is only one Hub), the easiest way is to configure a VPN star community in R80 SmartConsole:
1. On the **Star Community** window, in the:
a. Center Gateways section, select the Security Gateway that functions as the "Hub".
b. Satellite Gateways section, select Security Gateways as the "spokes", or satellites.
2. On the **VPN Routing** page, **Enable VPN routing for satellites** section, select one of these options:

a. **To center and to other Satellites through center -** This allows connectivity between the Security Gateways, for example if the spoke Security Gateways are DAIP Security Gateways, and the Hub is a Security Gateway with a static IP address.
b. **To center, or through the center to other satellites, to internet and other VPN targets -** This allows connectivity between the Security Gateways as well as the ability to inspect all communication passing through the Hub to the Internet.
3. Create an appropriate Access Control Policy rule.
4. NAT the satellite Security Gateways on the Hub if the Hub is used to route connections from Satellites to the Internet.
The two Dynamic Objects (DAIP Security Gateways) can securely route communication through the Security Gateway with the static IP address.

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

QUESTION 70
What is the default shell of Gaia CLI?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
This chapter gives an introduction to the Gaia command line interface (CLI).
The default shell of the CLI is called `clish`.
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm

QUESTION 71
Which of the following licenses are considered temporary?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 72
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 73
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 74
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 75

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 76
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 77

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 78
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 79
Which Check Point software blade provides protection from zero-day and undiscovered threats?

A. Firewall
B. Threat Emulation

C. Application Control

D. Threat Extraction

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

A. assign privileges to users.

B. edit the home directory of the user.

C. add users to your Gaia system.

D. assign user rights to their home directory in the Security Management Server

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Users
Use the WebUI and CLI to manage user accounts. You can:

- Add users to your Gaia system.
- Edit the home directory of the user.
- Edit the default shell for a user.
- Give a password to a user. ▪
Give privileges to users.

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

QUESTION 81

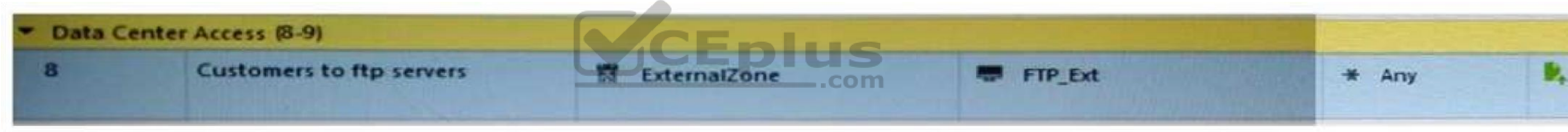
Look at the following screenshot and select the BEST answer.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Fill in the blanks: A security Policy is created in _________ , stored in the _________ , and Distributed to the various __________ .



Data Center Access (8-9)

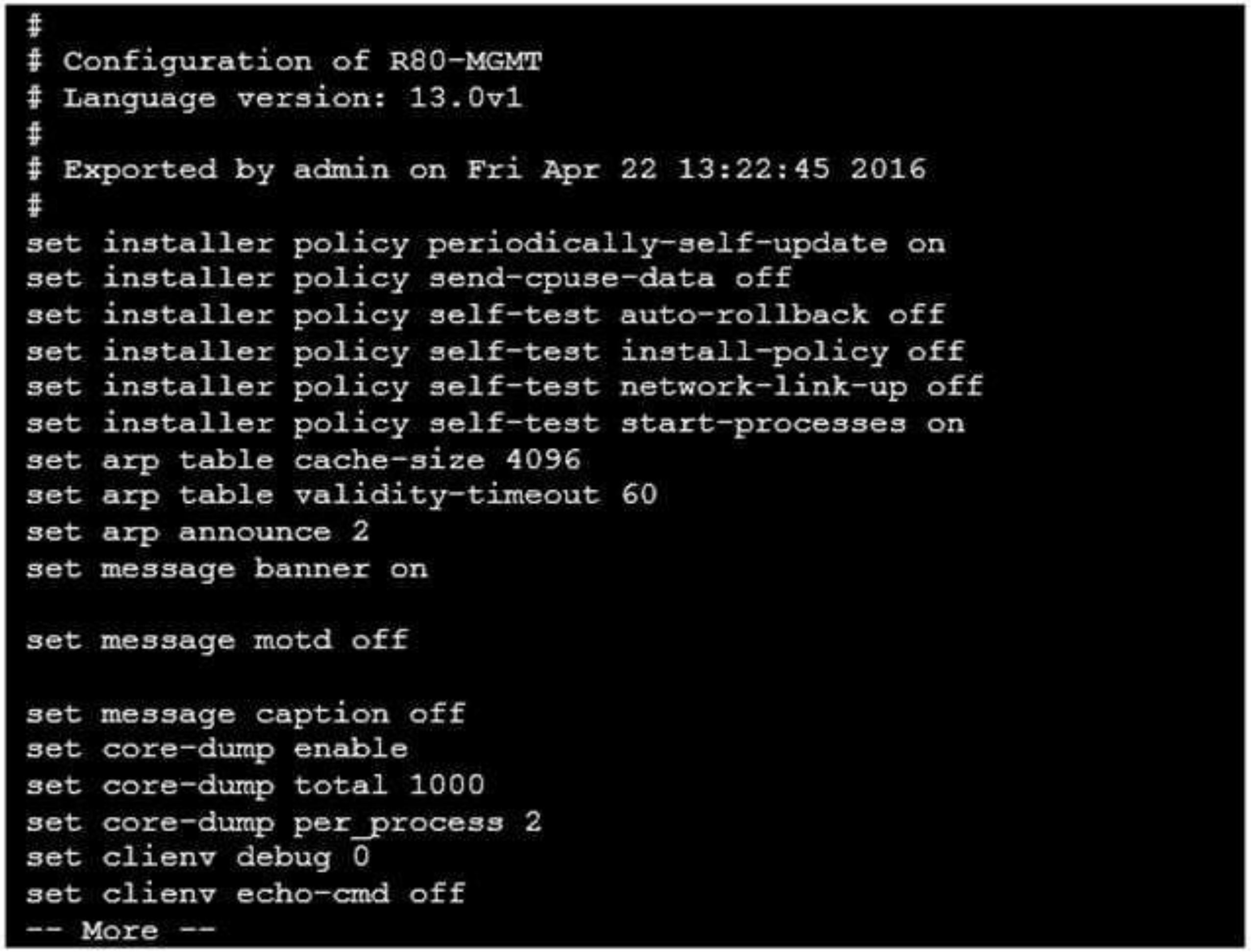
8	Customers to ftp servers	ExternalZone	FTP_Ext	Any

A. Rule base, Security Management Server, Security Gateways B.
SmartConsole, Security Gateway, Security Management Servers
C. SmartConsole, Security Management Server, Security Gateways
D. The Check Point database, SmartConsole, Security Gateways

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Look at the screenshot below. What CLISH command provides this output?



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

set message motd off

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

A. show configuration all

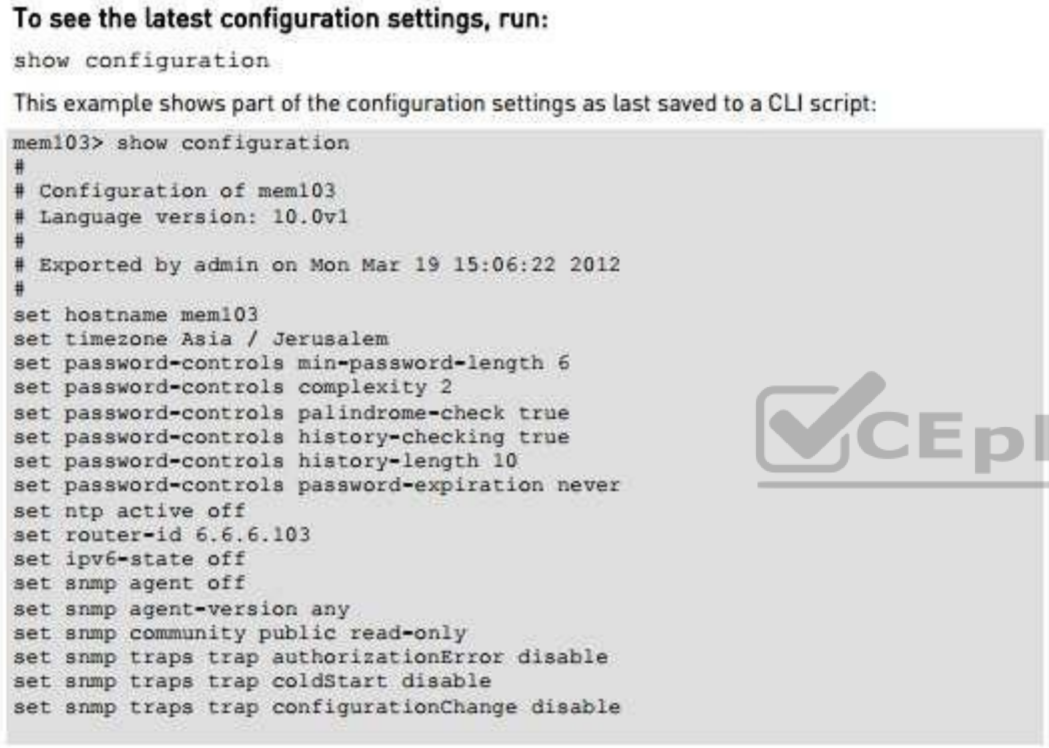
B. show confd configuration

C. show confd configuration all

D. `show configuration`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:



To see the latest configuration settings, run:

```
show configuration
```

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

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

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

QUESTION 84
Which authentication scheme requires a user to possess a token?

A. TACACS
B. SecurID
C. Check Point password

D. RADIUS

Correct Answer: B
Section: (none)
Explanation

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

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

QUESTION 85
If there is an Accept Implied Policy set to “First”, what is the reason Jorge cannot see any logs?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 86
The most important part of a site-to-site VPN deployment is the ________ .

A. Internet
B. Remote users
C. Encrypted VPN tunnel
D. VPN gateways

Correct Answer: C
Section: (none)

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

QUESTION 87
R80 Security Management Server can be installed on which of the following operating systems?

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

Correct Answer: A
Section: (none)
Explanation

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

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

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

QUESTION 88
What port is used for delivering logs from the gateway to the management server?

A. Port 258

B. Port 18209
C. Port 257
D. Port 981

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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:
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:
Explanation:
These users are created by default and cannot be deleted:

- **admin** — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user has a User ID of 0, and therefore has all of the privileges of a root user.
- **monitor** — Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.

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

QUESTION 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

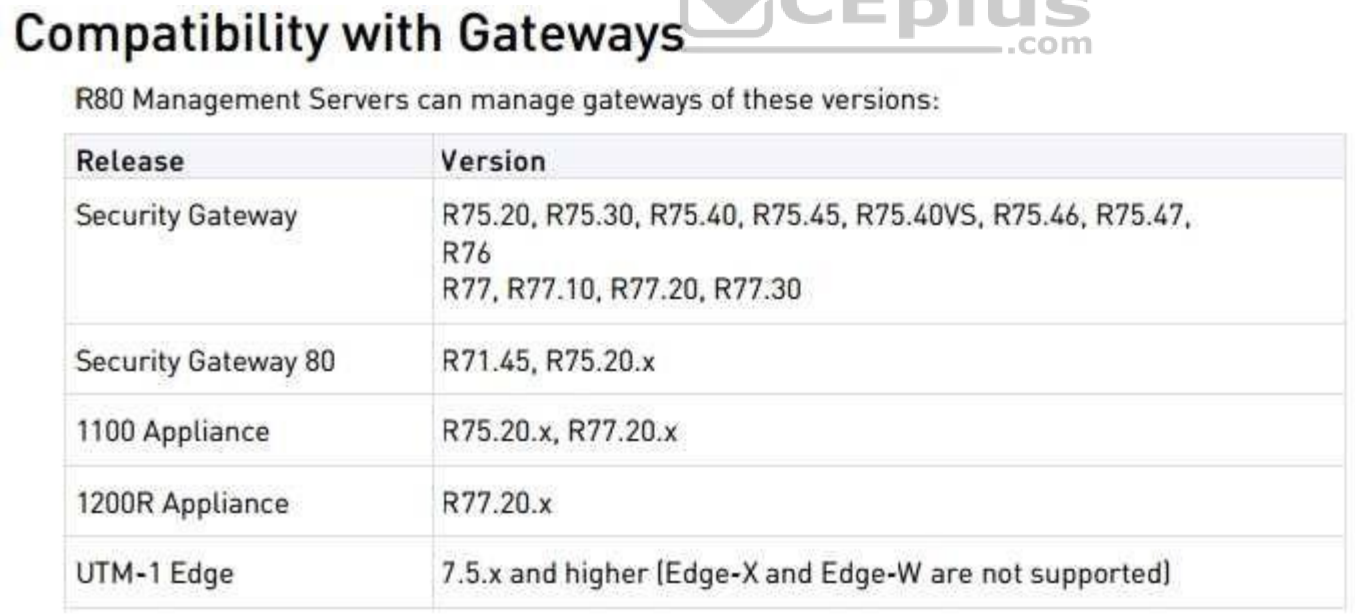
Explanation/Reference:
Explanation:
Snapshot Management
The snapshot creates a binary image of the entire root (*lv_current*) disk partition. This includes Check Point products, configuration, and operating system.
Starting in **R77.10**, exporting an image from one machine and importing that image on 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

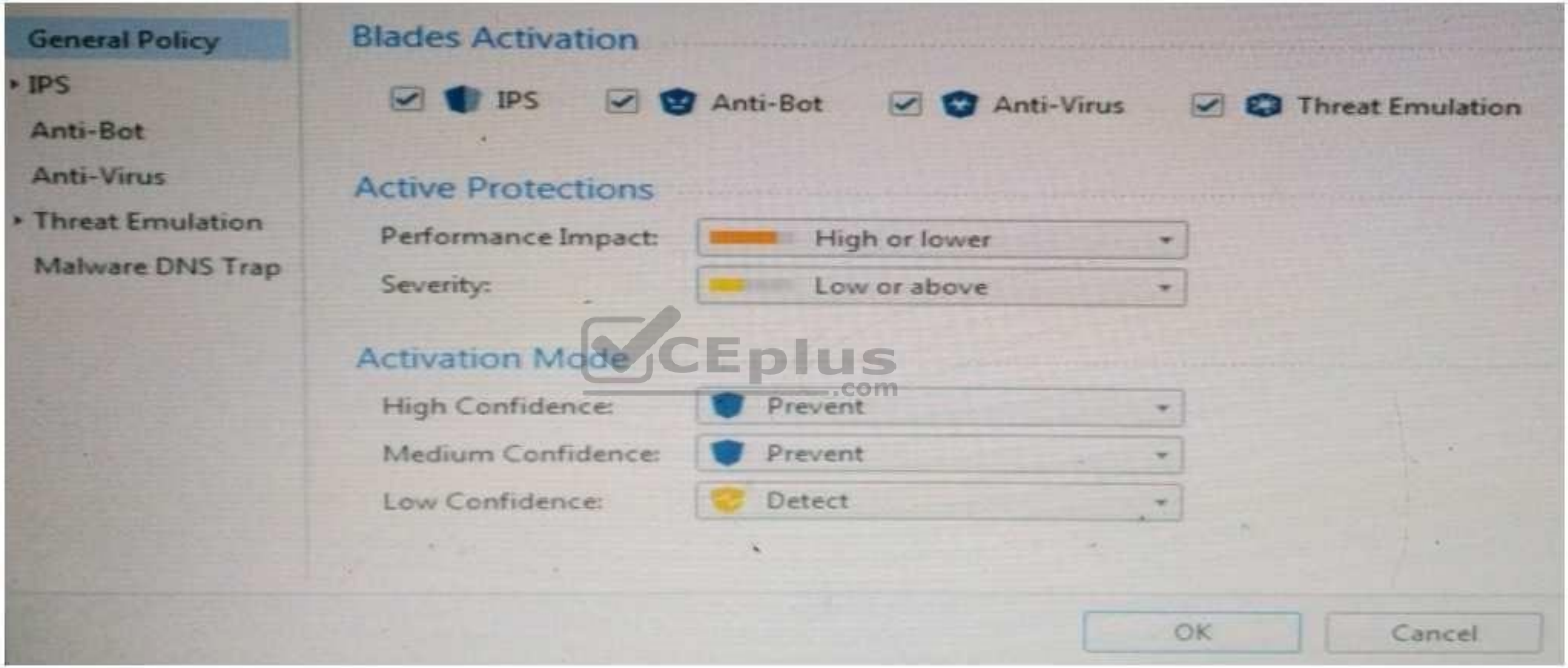
R80 Management Servers can manage gateways of these versions:

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.

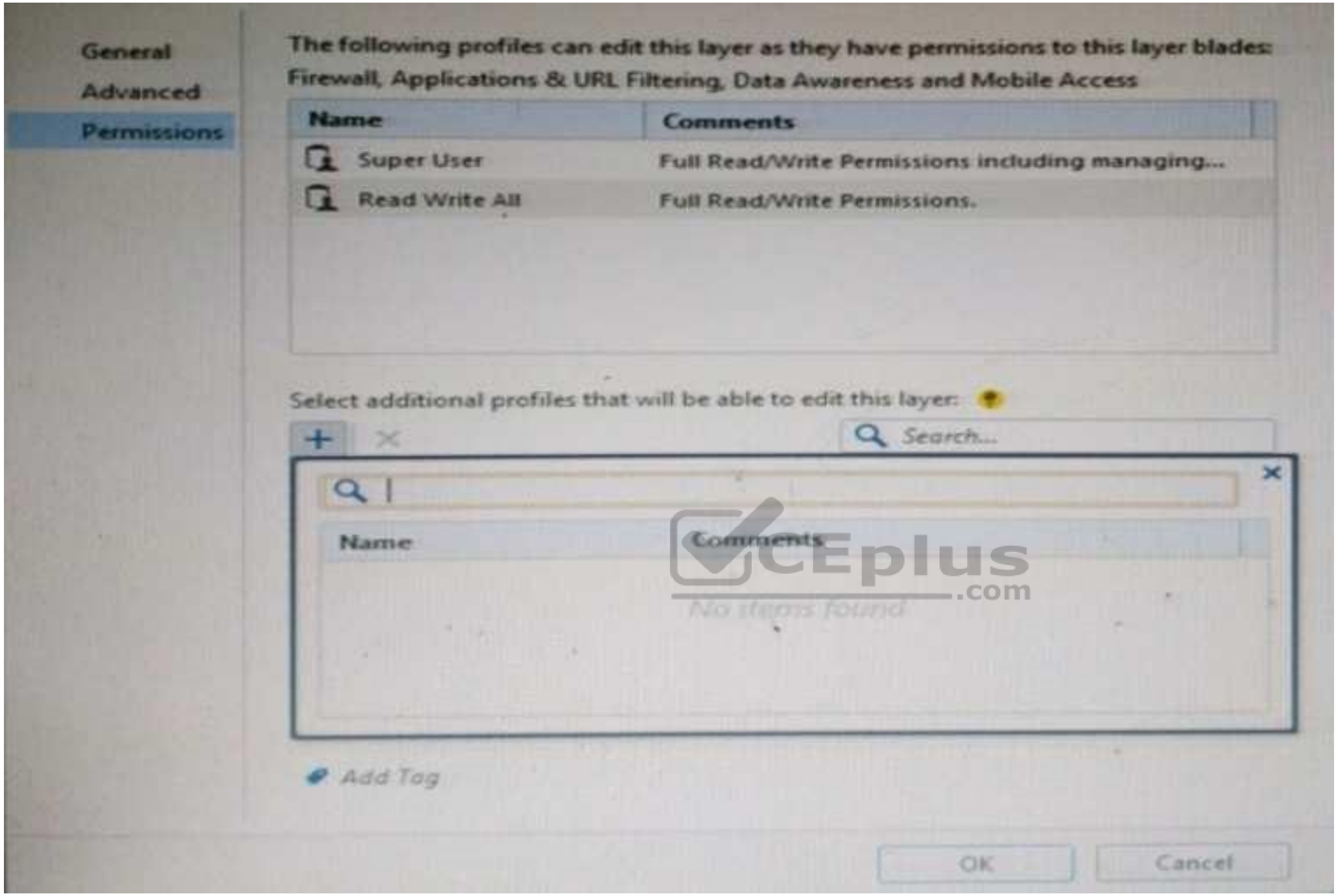
A. Shared policy packages
B. Shared policies
C. Concurrent policy packages
D. Concurrent policies

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

No items found

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 of the following statements accurately describes the command `snapshot`?

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

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

QUESTION 103

The Captive Portal tool:

A. Acquires identities from unidentified users.
B. Is only used for guest user authentication.
C. Allows access to users already identified.
D. Is deployed from the Identity Awareness page in the Global Properties settings.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104

Where do we need to reset the SIC on a gateway object?

A. SmartDashboard > Edit Gateway Object > General Properties > Communication
B. SmartUpdate > Edit Security Management Server Object > SIC
C. SmartUpdate > Edit Gateway Object > Communication
D. SmartDashboard > Edit Security Management Server Object > SIC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
What happens if the identity of a user is known?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Message digests use which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 108
When using LDAP as an authentication method for Identity Awareness, the query:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

A. The POP3 rule is disabled.
B. POP3 is accepted in **Global Properties**.
C. The POP3 rule is hidden.
D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
What action can be performed from SmartUpdate R77?

A. `upgrade_export`
B. `fw stat -1`
C. `cpinfo`
D. `remote_uninstall_verifier`

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Your manager requires you to setup a VPN to a new business partner site. The administrator from the partner site gives you his VPN settings and you notice that he setup AES 128 for IKE phase 1 and AES 256 for IKE phase 2. Why is this a problematic setup?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Choose the SmartLog property that is TRUE.

A. SmartLog has been an option since release R71.10.
B. SmartLog is not a Check Point product.
C. SmartLog and SmartView Tracker are mutually exclusive.
D. SmartLog is a client of SmartConsole that enables enterprises to centrally track log records and security activity with Google-like search.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 113
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 114
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 115
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 116
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 117
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

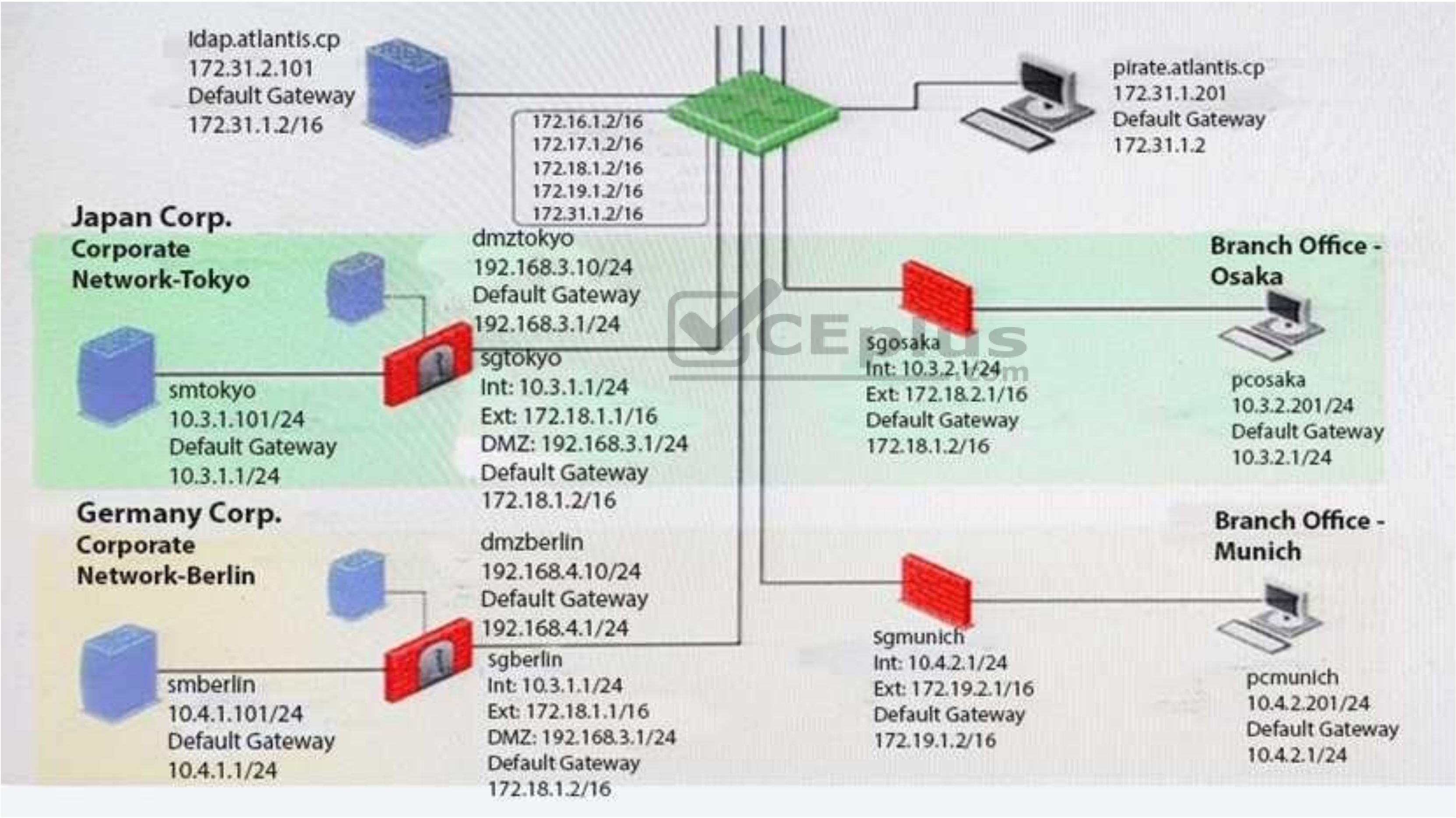
Correct Answer: B

Section: (none)
Explanation

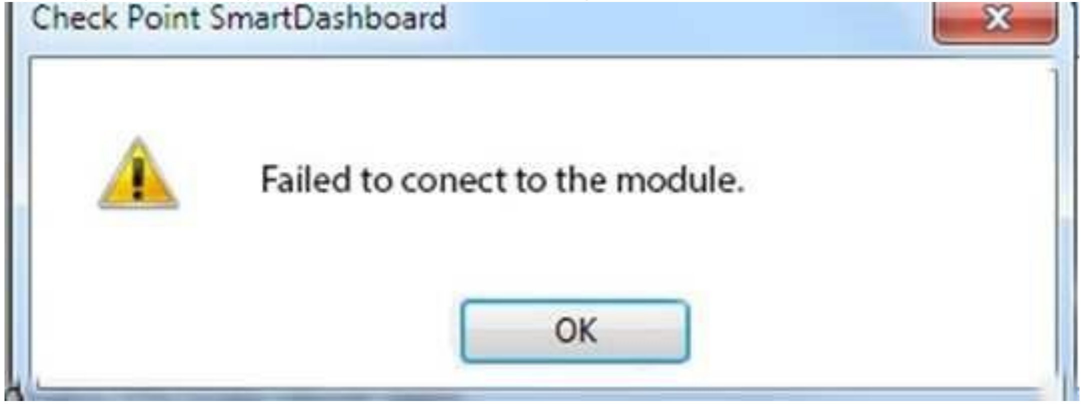
Explanation/Reference:

QUESTION 118

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 119
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 120
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 121
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 122

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 123
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 124
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 125
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 126
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.

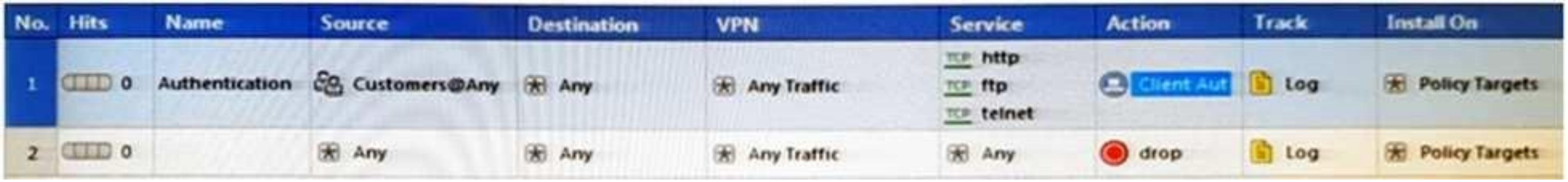
A. In the SmartView Tracker, if you activate the column **Matching Rate**.
B. In SmartReporter, in the section **Firewall Blade – Activity > Network Activity** with information concerning **Top Matched Logged Rules**.
C. SmartReporter provides this information in the section **Firewall Blade – Security > 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

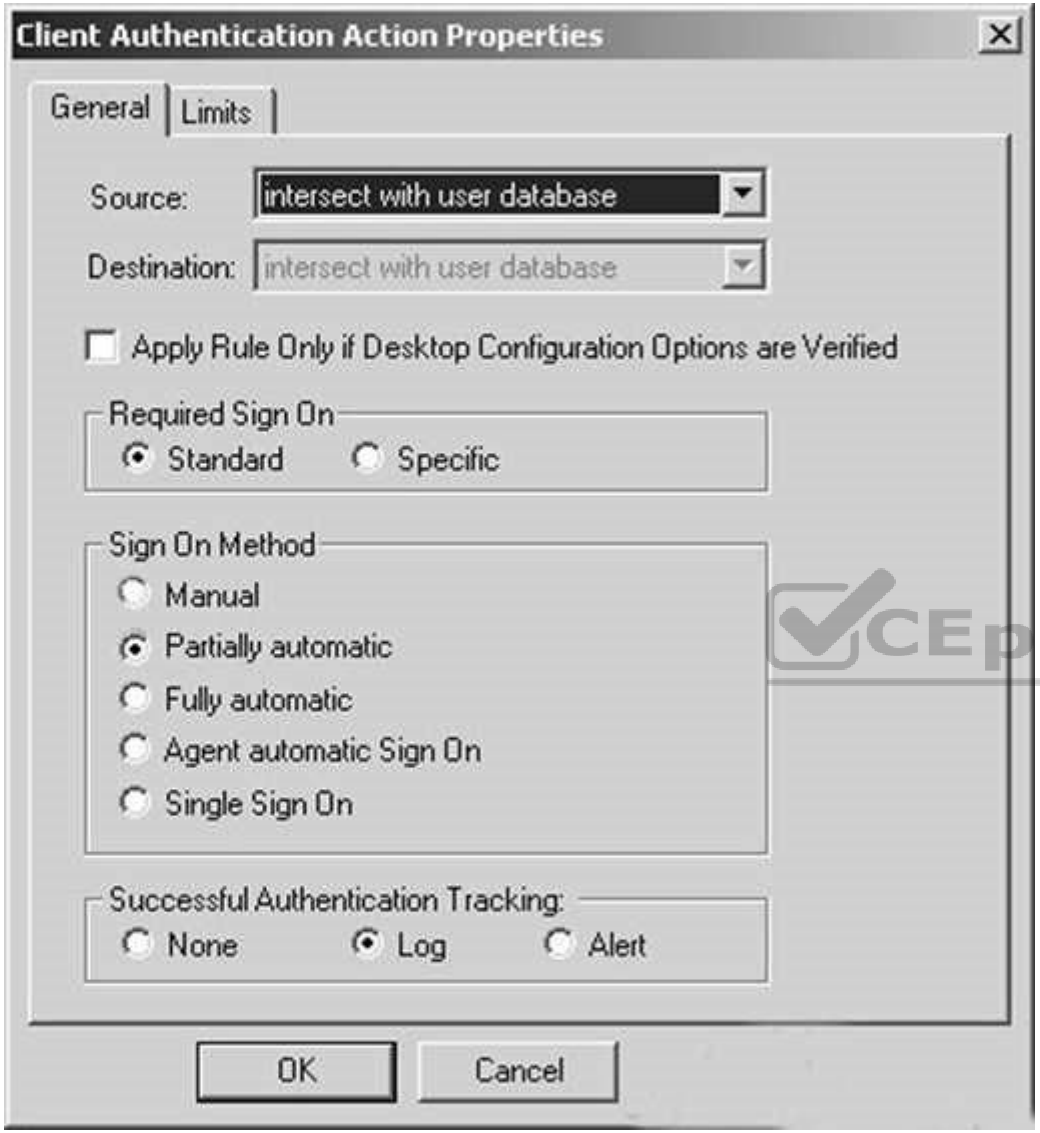
Explanation/Reference:

QUESTION 127

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

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 128
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 129
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 130
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:

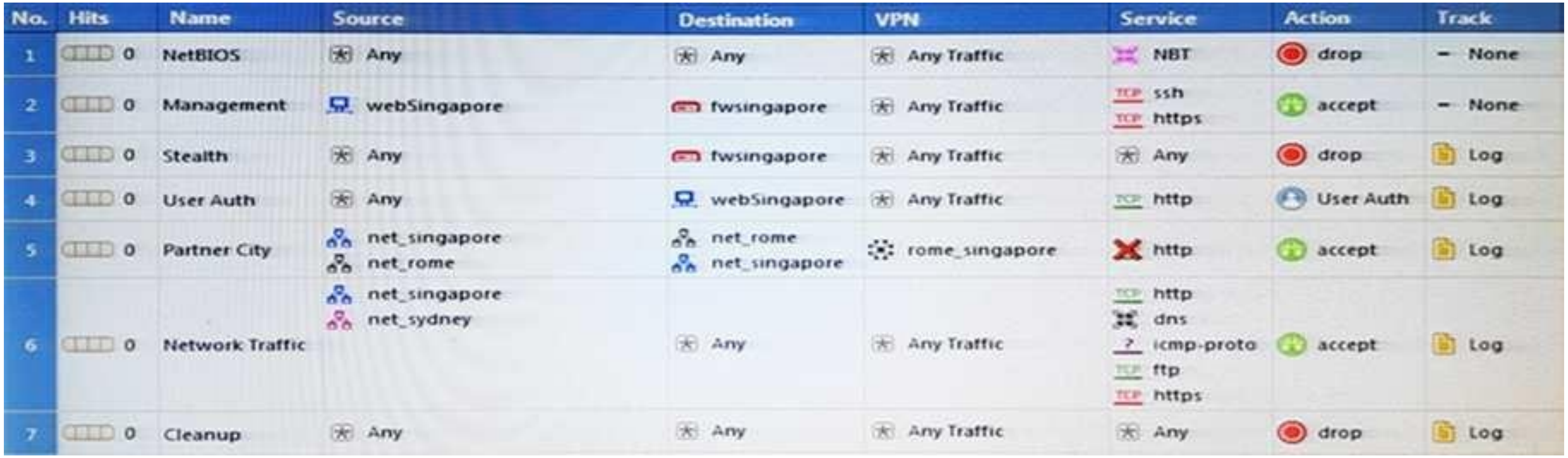
QUESTION 131
Which set of objects have an **Authentication** tab?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
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 133
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 134
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 135
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 136

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 137

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 138

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

A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status

B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor

C. SmartView Tracker, CPINFO, SmartUpdate

D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139

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 140

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 141

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 142

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 143

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 144
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 145
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 146

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 147

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 148

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 149

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 150

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 151

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 152

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

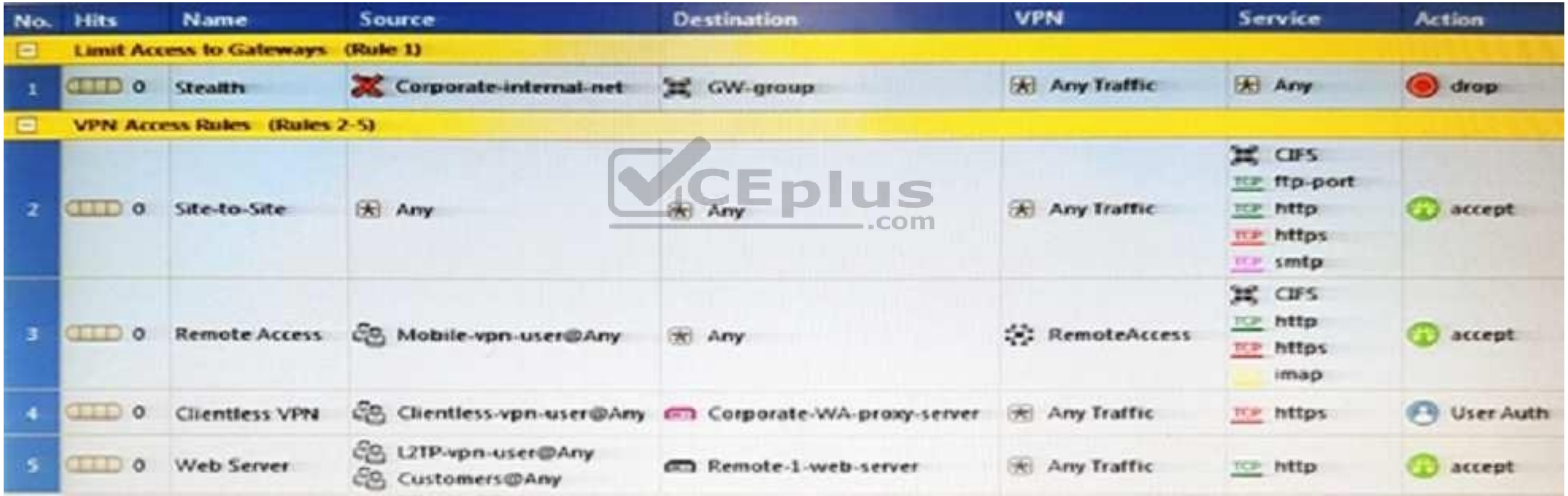
A. From the Internet

B. Through internal interfaces
C. Through all interfaces
D. According to the Firewall Policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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 154
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 155
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 156
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 157
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 158
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 159

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 160

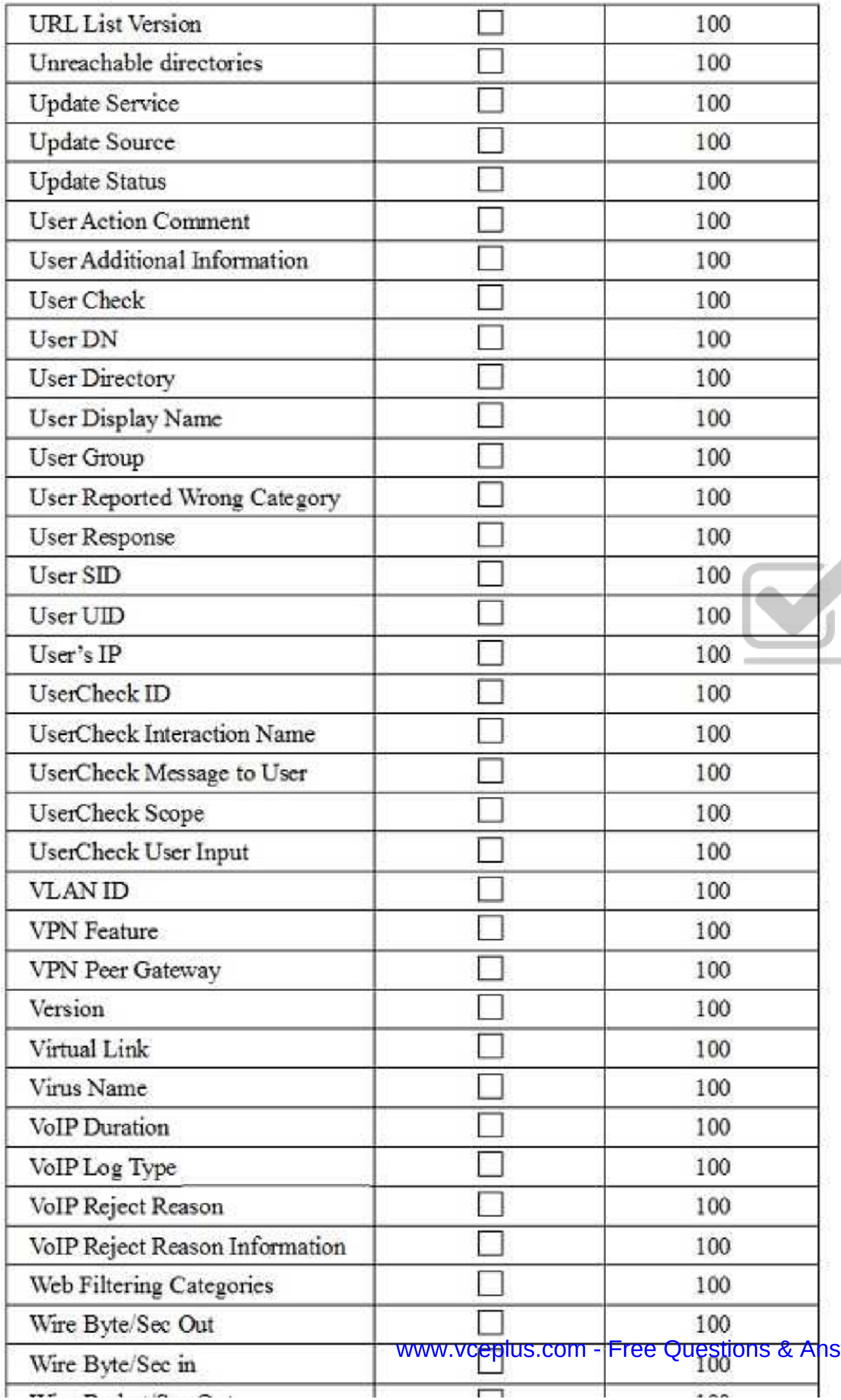
You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

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 161
You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?



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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
What happens if the identity of a user is known?

A. If the user credentials do not match an Access Role, the traffic is automatically dropped.
B. If the user credentials do not match an Access Role, the system displays a sandbox.
C. If the user credentials do not match an Access Role, the gateway moves onto the next rule.
D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Your company enforces a strict change control policy. Which of the following would be MOST effective for quickly dropping an attacker's specific active connection?

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 164
What port is used for communication to the User Center with SmartUpdate?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
How do you configure an alert in SmartView Monitor?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
Where would an administrator enable Implied Rules logging?

A. In Smart Log Rules View
B. In SmartDashboard on each rule
C. In Global Properties under Firewall
D. In Global Properties under log and alert

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

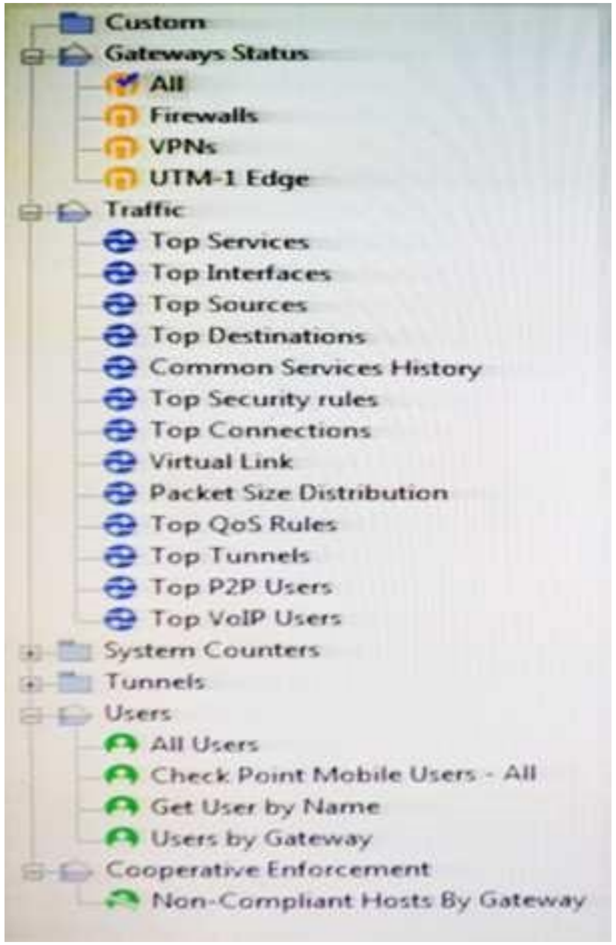
QUESTION 167
Which of these attributes would be critical for a site-to-site VPN?

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

Correct Answer: D
Section: (none)
Explanation

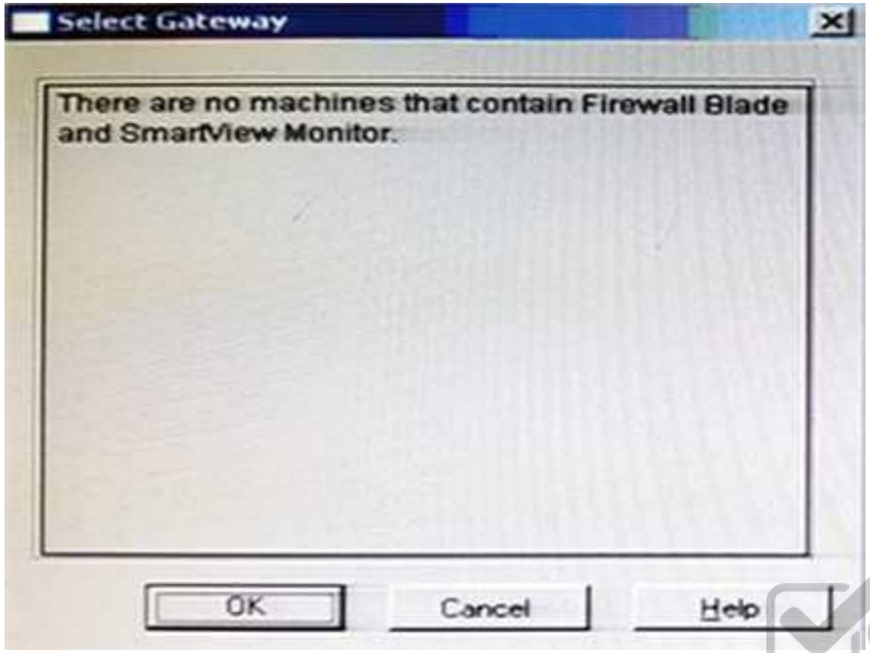
Explanation/Reference:

QUESTION 168
You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.



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

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



Select Gateway

There are no machines that contain Firewall Blade and SmartView Monitor.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners. Which SmartConsole application should you use to confirm your suspicious?

A. SmartDashboard

B. SmartUpdate
C. SmartView Status
D. SmartView Tracker

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
Which of the following uses the same key to decrypt as it does to encrypt?

A. Asymmetric encryption
B. Dynamic encryption
C. Certificate-based encryption
D. Symmetric encryption

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
How do you configure the Security Policy to provide uses access to the Captive Portal through an external (Internet) interface?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172

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

A. You can only use the rule for Telnet, FTP, SMPT, and rlogin services.

B. The Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.

C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.

D. You can limit the authentication attempts in the **User Properties' Authentication** tab.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173

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 174

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 175
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 176
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 177

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 178

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 179

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 180
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 181
How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Reference: http://dl3.checkpoint.com/paid/f2/f2faf02dba06acad8cc4c57833593df6/CP_TE100X_TE250X_Appliance_GettingStartedGuide.pdf?

HashKey=1517091196_a292abdde351bbdb4b3d28e82654b240&xtn=.pdf

QUESTION 182
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 183
Identify the API that is not supported by Check Point currently.

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 184
Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 185
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 186
Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?

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

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

QUESTION 187
What is the command to see cluster status in cli expert mode?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 189
If the first packet of an UDP session is rejected by a security policy, what does the firewall send to the client?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
What is the mechanism behind Threat Extraction?

A. This is a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender
B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient
C. This is a new mechanism to identify the IP address of the sender of malicious codes and to put it into the SAM database (Suspicious Activity Monitoring).
D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
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 192

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 193

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 194

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 195
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: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
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 197
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 198
What command would show the API server status?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
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 200
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 201
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 202
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 203
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 204
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 205

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 206

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 207

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 208

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 209

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 210

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 211

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 212
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 213
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 214
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 215
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 216
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 217
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 218
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 219
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: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 220
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 221

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 222
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 223
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 224
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 225
Fill in the blank: An LDAP server holds one or more ______________.

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

Correct Answer: C
Section: (none)
Explanation

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

CP_R77_SecurityManagement_WebAdminGuide/94041

QUESTION 226

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 227

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 228

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 229
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 230
Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 231
Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 232
What is the Transport layer of the TCP/IP model responsible for?

A. It transports packets as datagrams along different routes to reach their destination.
B. It manages the flow of data between two hosts to ensure that the packets are correctly assembled and delivered to the target application.
C. It defines the protocols that are used to exchange data between networks and how host programs interact with the Application layer.
D. It deals with all aspects of the physical components of network connectivity and connects with different network types.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 233
What needs to be configured if the NAT property ‘Translate destination on client side’ is not enabled in Global properties?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 234
In the Check Point Security Management Architecture, which component(s) can store logs?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 235
Fill in the blank: In order to install a license, it must first be added to the ____________.

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

Correct Answer: B

Section: (none)
Explanation

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

QUESTION 236
When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 237
Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the ____________ algorithm.

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

Correct Answer: A
Section: (none)
Explanation

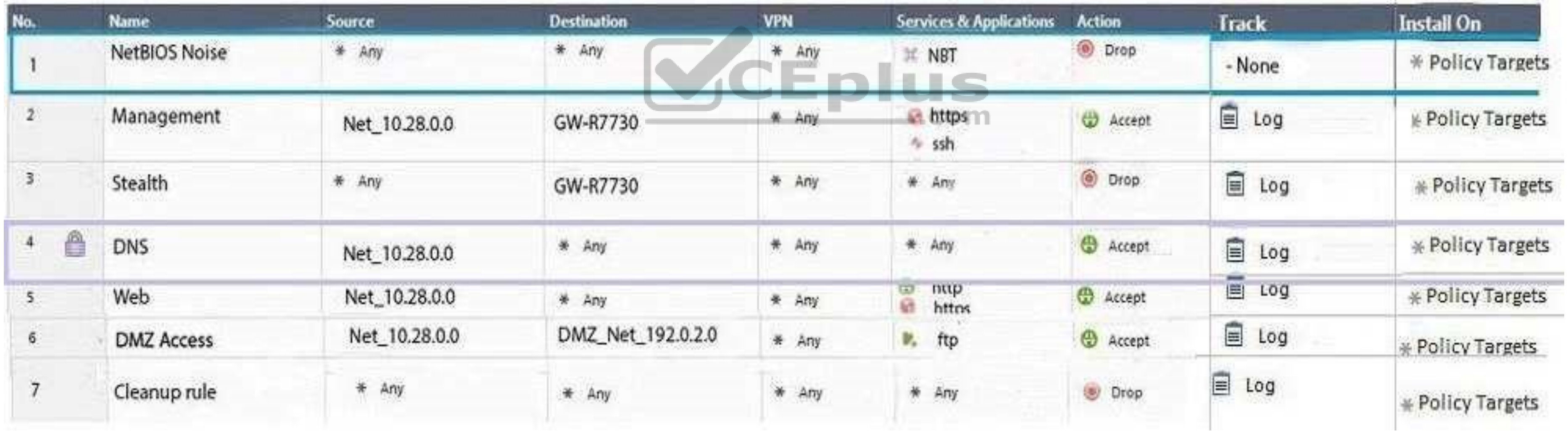
Explanation/Reference:

QUESTION 238
Which message indicates IKE Phase 2 has completed successfully?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 239
Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	- None	* Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh	Accept	Log	* Policy Targets
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	Log	* Policy Targets
4 🔒	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	Log	* Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http https	Accept	Log	* Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	Accept	Log	* Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	* Policy Targets

What is the possible explanation for this?

A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
B. Another administrator is logged into the Management and currently editing the DNS Rule.
C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.

D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 240
Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays _____________ for the given VPN tunnel.

A. Down
B. No Response
C. Inactive
D. Failed

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 241
Which of the following is the most secure means of authentication?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 242

What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

A. `ifconfig -a`

B. `show interfaces`

C. `show interfaces detail`

D. `show configuration interface`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 243

Fill in the blank: Authentication rules are defined for ____________.

A. User groups
B. Users using UserCheck
C. Individual users
D. All users in the database

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 244

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

A. ThreatWiki
B. Whitelist Files

C. AppWiki
D. IPS Protections

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 245
Which of the following is an authentication method used for Identity Awareness?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 246
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 247

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 248

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 249
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 250
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 251
You have discovered suspicious activity in your network. What is the BEST immediate action to take?

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

Correct Answer: B
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/118300

QUESTION 252
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 253
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 254
How would you determine the software version from the CLI?

A. `fw ver`

B. `fw stat`

C. `fw monitor`

D. `cpinfo`

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

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

B. Add `tcpdump` to CLISH using `add command`.
Create a new access role.

Add `tcpdump` to the role.
Create new user with UID 0 and assign role to the user.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24
set static-route default nexthop gateway address 192.168.80.1 on
save config

B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0
add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 on save config

C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0
add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 on save config

D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24
add static-route default nexthop gateway address 192.168.80.1
on save config

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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

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

Correct Answer: B
Section: (none)
Explanation

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

A. Allows the administrator to share a policy between all the users identified by the Security Gateway
B. Allows the administrator to share a policy between all the administrators managing the Security Management Server

C. Allows the administrator to share a policy so that it is available to use in another Policy Package
D. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 260
What is the purpose of a Clean-up Rule?

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

Correct Answer: C
Section: (none)
Explanation

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

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

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

QUESTION 261
What are the two types of NAT supported by the Security Gateway?

A. Destination and Hide
B. Hide and Static
C. Static and Source
D. Source and Destination

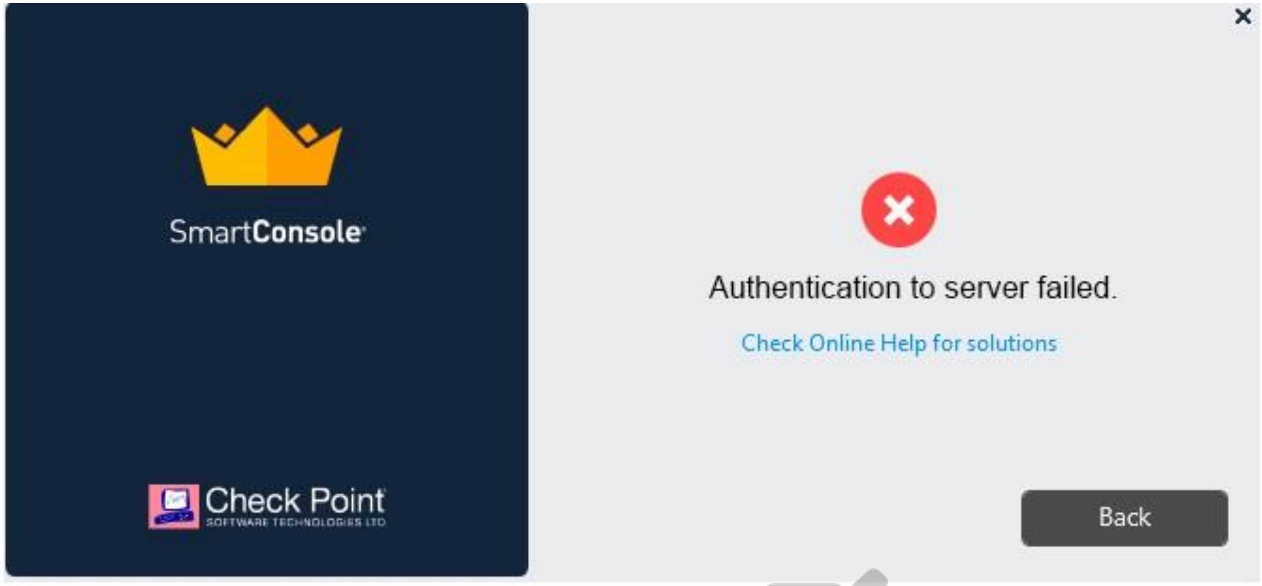
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A Security Gateway can use these procedures to translate IP addresses in your network:

- **Static NAT** - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.
- **Hide NAT** - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers, external computers CANNOT access internal servers. The Firewall can translate up to 50,000 connections at the same time from external computers and servers.
- **Hide NAT with Port Translation** - Use one IP address and let external users access multiple application servers in a hidden network. The Firewall uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules to use Port Translation.

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

QUESTION 262
Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.



Authentication to server failed.

Check Online Help for solutions

What is the most likely reason?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 263
What is the most complete definition of the difference between the Install Policy button on the SmartConsole's tab, and the Install Policy within a specific policy?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 264
John is the administrator of a R80 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John's changes available to other administrators, and to save the database before installing a policy, what must John do?

A. Logout of the session
B. **File > Save**
C. Install database
D. Publish the session

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Installing and Publishing

It is important to understand the differences between publishing and installing.

You must do this:	After you did this:
Publish	Opened a session in SmartConsole and made changes. The Publish operation sends all SmartConsole modifications to other administrators, and makes the changes you made in a private session public.
Install the database	Modified network objects, such as servers, users, services, or IPS profiles, but not the Rule Base. Updates are installed on management servers and log servers.
Install a policy	Changed the Rule Base. The Security Management Server installs the updated policy and the entire database on Security Gateways (even if you did not modify any network objects).

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/119225

QUESTION 265

Fill in the blanks: There are ________ types of software containers ________.

A. Three; security management, Security Gateway, and endpoint security
B. Three; Security gateway, endpoint security, and gateway management
C. Two; security management and endpoint security
D. Two; endpoint security and Security Gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

There are three **types of Software Containers**: Security Management, Security Gateway, and Endpoint Security.

Reference:
http://downloads.checkpoint.com/dc/download.htm?ID=11608

QUESTION 266

Fill in the bank: In Office mode, a Security Gateway assigns a remote client to an IP address once___________.

A. the user connects and authenticates

B. office mode is initiated

C. the user requests a connection

D. the user connects

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Office Mode enables a Security Gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates. The assignment lease is renewed as long as the user is connected.

Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13857.htm

QUESTION 267

Which Identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

A. AD Query

B. Terminal Servers Endpoint Identity Agent

C. Endpoint Identity Agent and Browser-Based Authentication

D. RADIUS and Account Logon

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Endpoint Identity Agents and **Browser-Based Authentication -** When a high level of security is necessary. The Captive Portal is used for distributing the Endpoint Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

Reference:

https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/101858

QUESTION 268
What is the most recommended installation method for Check Point appliances?

A. SmartUpdate installation
B. DVD media created with Check Point ISOMorphic
C. USB media created with Check Point ISOMorphic
D. Cloud based installation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 269
Which of the following is NOT a role of the SmartCenter:

A. Status monitoring
B. Policy configuration
C. Certificate authorityD. Address translation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: www.checkfirewalls.com/datasheets/smartcenter_datasheet.pdf

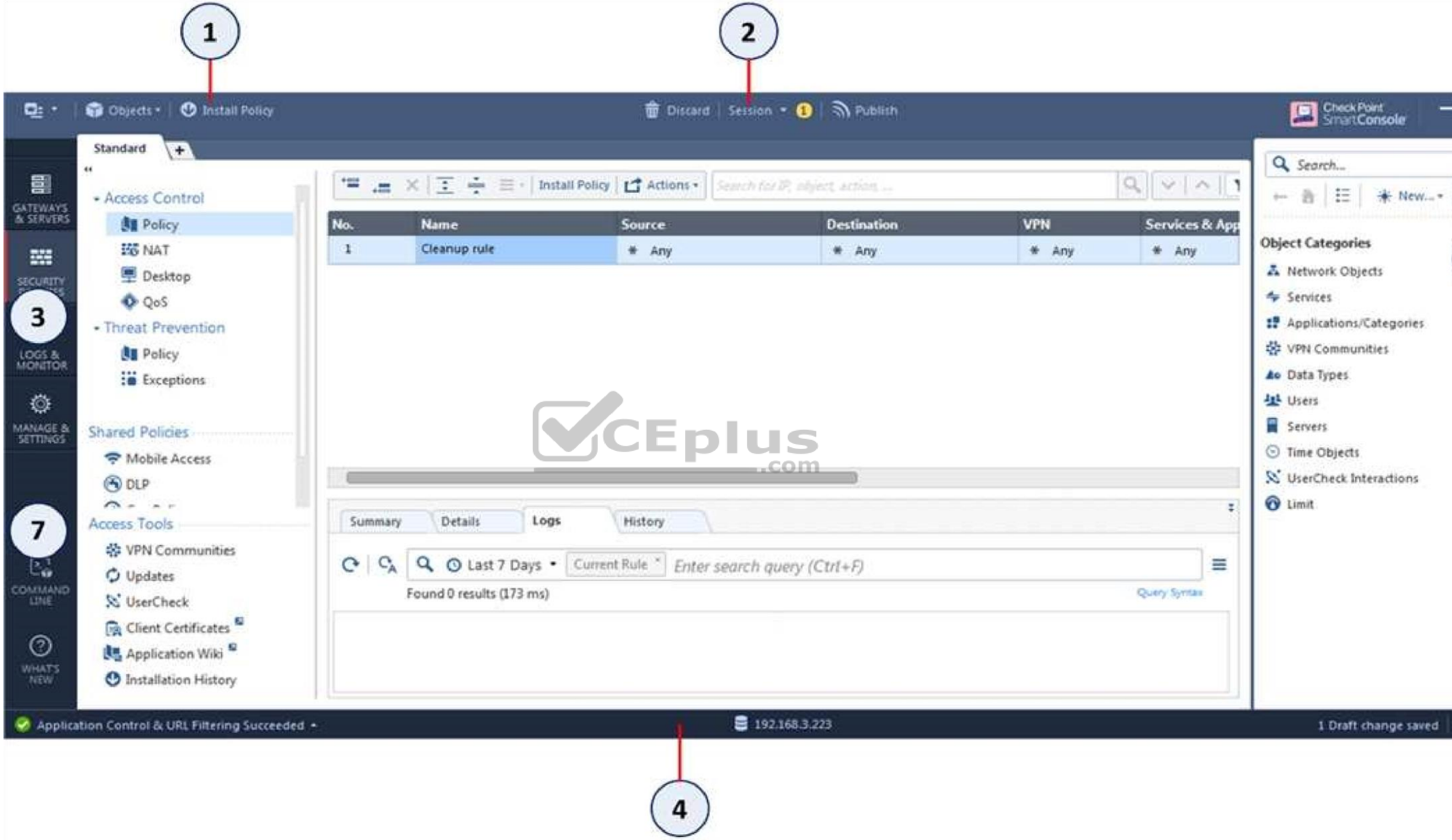
QUESTION 270
Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

A. Manage and Command Line
B. Logs and Monitor
C. Security Policies

D. Gateway and Servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:



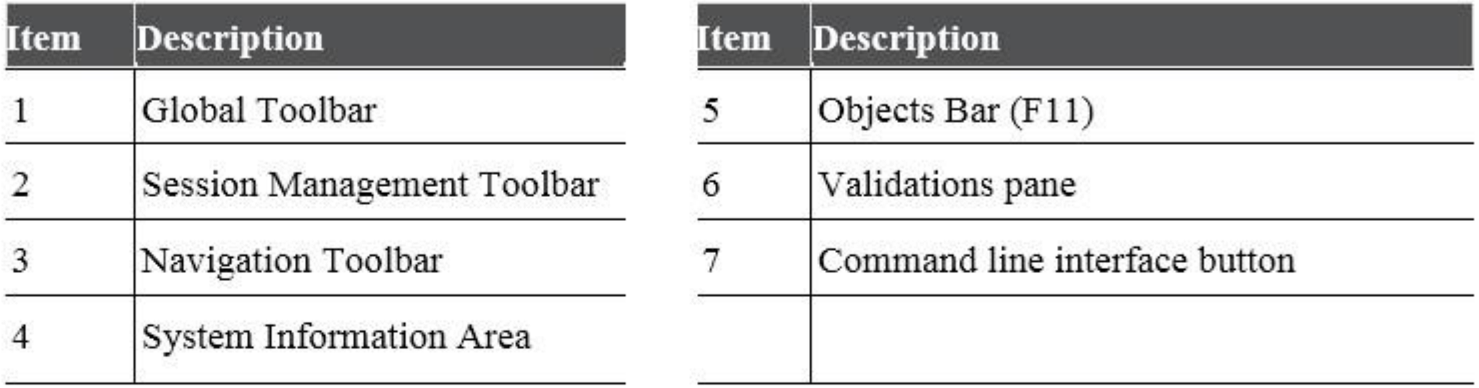
No.	Name	Source	Destination	VPN	Services & App
1	Cleanup rule	Any	Any	Any	Any

Found 0 results (173 ms)

Application Control & URL Filtering Succeeded

192.168.3.223

1 Draft change saved



Item	Description
1	Global Toolbar
2	Session Management Toolbar
3	Navigation Toolbar
4	System Information Area

Item	Description
5	Objects Bar (F11)
6	Validations pane
7	Command line interface button

Reference: https://sc1.checkpoint.com/documents/R80.10/SmartConsole_OLH/EN/html_frameset.htm?topic=documents/R80.10/SmartConsole_OLH/EN/4x3HIUbSkxYhtcFgIKlg0w2

QUESTION 271

What is the BEST method to deploy Identity Awareness for roaming users?

A. Use Office Mode
B. Use identity agents
C. Share user identities between gateways
D. Use captive portal

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Using Endpoint Identity Agents give you: ▪
User and machine identity

- *Minimal user intervention* – all necessary configuration is done by administrators and does not require user input.
- *Seamless connectivity* – transparent authentication using Kerberos Single Sign-On (SSO) when users are logged in to the domain. If you do not want to use SSO, users enter their credentials manually. You can let them save these credentials.
- *Connectivity through roaming* – users stay automatically identified when they move between networks, as the client detects the movement and reconnects.

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

QUESTION 272
What is the purpose of the Clean-up Rule?

A. To log all traffic that is not explicitly allowed or denied in the Rule Base
B. To clean up policies found inconsistent with the compliance blade reports
C. To remove all rules that could have a conflict with other rules in the database
D. To eliminate duplicate log entries in the Security Gateway

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

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

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

QUESTION 273
Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

A. Application Control
B. Threat Emulation
C. Anti-Virus
D. Advanced Networking Blade

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 274

Fill in the blank: Back up and restores can be accomplished through_________.

A. SmartConsole, WebUI, or CLI

B. WebUI, CLI, or SmartUpdate

C. CLI, SmartUpdate, or SmartBackup

D. SmartUpdate, SmartBackup, or SmartConsole

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Backup and Restore
These options let you:

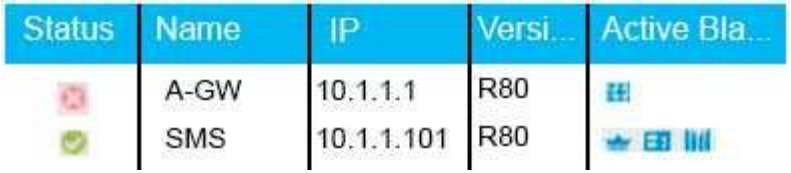
- Back up the Gaia OS configuration and the firewall database to a compressed file
- Restore the Gaia OS configuration and the firewall database from a compressed file To back up a configuration:

1. Right-click the Security Gateway.
2. Select **Backup and Restore > Backup**. The **Backup** window opens.
3. Select the backup location.

Reference: https://community.checkpoint.com/thread/5375-checkpoint-gateway-firewall-backup-through-smart-console

QUESTION 275

What does it mean if Deyra sees the gateway status:



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

Choose the BEST answer.

A. SmartCenter Server cannot reach this Security Gateway

B. There is a blade reporting a problem

C. VPN software blade is reporting a malfunction

D. Security Gateway’s MGNT NIC card is disconnected.

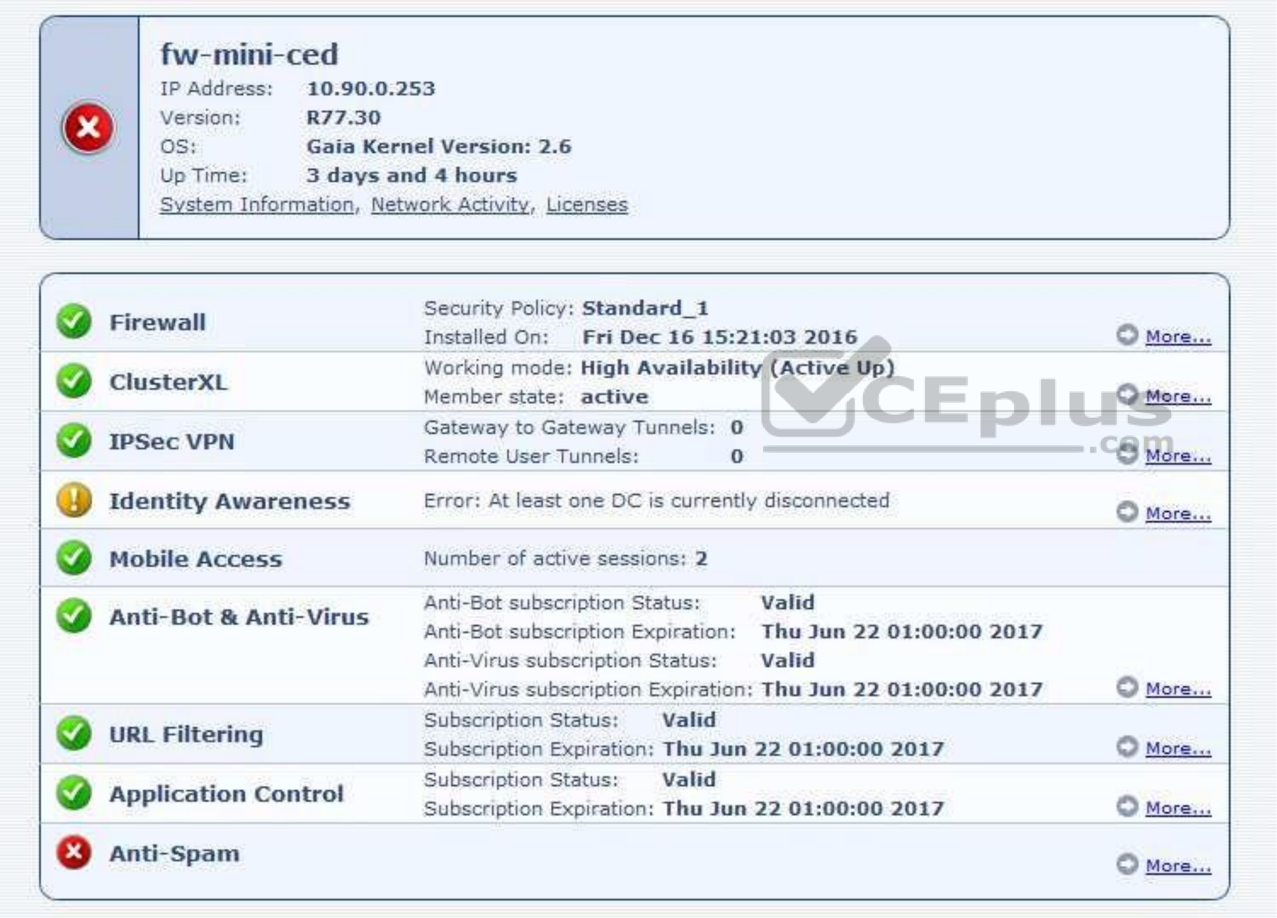
Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:



✗ **fw-mini-ced**

IP Address:	10.90.0.253
Version:	R77.30
OS:	Gaia Kernel Version: 2.6
Up Time:	3 days and 4 hours

System Information, Network Activity, Licenses

✓	Firewall	Security Policy: Standard_1 Installed On: Fri Dec 16 15:21:03 2016	More...
✓	ClusterXL	Working mode: High Availability (Active Up) Member state: active	More...
✓	IPSec VPN	Gateway to Gateway Tunnels: 0 Remote User Tunnels: 0	More...
!	Identity Awareness	Error: At least one DC is currently disconnected	More...
✓	Mobile Access	Number of active sessions: 2	
✓	Anti-Bot & Anti-Virus	Anti-Bot subscription Status: Valid Anti-Bot subscription Expiration: Thu Jun 22 01:00:00 2017 Anti-Virus subscription Status: Valid Anti-Virus subscription Expiration: Thu Jun 22 01:00:00 2017	More...
✓	URL Filtering	Subscription Status: Valid Subscription Expiration: Thu Jun 22 01:00:00 2017	More...
✓	Application Control	Subscription Status: Valid Subscription Expiration: Thu Jun 22 01:00:00 2017	More...
✗	Anti-Spam		More...

Reference: https://sc1.checkpoint.com/sc/SolutionsStatics/NEW_SK_NOID1493612962436/active1704302237.fw.png **QUESTION 276**

When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

A. Distributed
B. Standalone
C. Bridge

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 277
One of major features in R80 SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

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

Correct Answer: C
Section: (none)
Explanation

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

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

QUESTION 278
When should you generate new licenses?

A. Before installing contract files.

B. After an RMA procedure when the MAC address or serial number of the appliance changes.

C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.
D. Only when the license is upgraded.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 279
Fill in the blank: When a policy package is installed, ________ are also distributed to the target installation Security Gateways.

A. User and objects databases
B. Network databases
C. SmartConsole databases
D. User databases

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

- **Access Control** - consists of these types of rules**:**
  - Firewall
  - NAT
  - Application Control and URL Filtering
  - Data Awareness
- **QoS**
- **Desktop Security** - the Firewall policy for endpoint computers that have the Endpoint Security VPN remote access client installed as a standalone client.
- **Threat Prevention** - consists of:
  - IPS - IPS protections continually updated by IPS Services
  - Anti-Bot - Detects bot-infected machines, prevents bot damage by blocking bot commands and Control (C&C) communications
  - Anti-Virus - Includes heuristic analysis, stops viruses, worms, and other malware at the gateway
  - Threat Emulation - detects zero-day and advanced polymorphic attacks by opening suspicious files in a sandbox

The installation process:

▪ Runs a heuristic verification on rules to make sure they are consistent and that there are no redundant rules.

If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

▪ Makes sure that each of the Security Gateways enforces at least one of the rules. If none of the rules are enforced, the default drop rule is enforced. ▪ Distributes the user database and object database to the selected installation targets.

Reference:
https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/119225

QUESTION 280

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

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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 281

How are the backups stored in Check Point appliances?

A. Saved as*.tar under /var/log/CPbackup/backups
B. Saved as*tgz under /var/CPbackup
C. Saved as*tar under /var/CPbackup
D. Saved as*tgz under /var/log/CPbackup/backups

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:
Backup configurations are stored in: /var/CPbackup/backups/

Reference:
https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/107104

QUESTION 282
You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

A. backup
B. logswitch
C. Database Revision
D. snapshot

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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 283
Which tool is used to enable ClusterXL?

A. SmartUpdate
B. cpconfig
C. SmartConsole
D. sysconfig

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_ClusterXL_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_ClusterXL_WebAdminGuide/161105

QUESTION 284
What type of NAT is a one-to-one relationship where each host is translated to a unique address?

A. Source
B. Static
C. Hide
D. Destination

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 285
True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway

A. True, CLI is the prefer method for Licensing
B. False, Central License are handled via Security Management Server
C. False, Central License are installed via Gaia on Security Gateways
D. True, Central License can be installed with CPLIC command on a Security Gateway

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 286

Which of the following is NOT an identity source used for Identity Awareness?

A. Remote Access
B. UserCheck
C. AD Query
D. RADIUS

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 287
Fill in the blanks: Default port numbers for an LDAP server is ______ for standard connections and _______ SSL connections.

A. 675, 389
B. 389, 636
C. 636, 290
D. 290, 675

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS.

QUESTION 288
Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?

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

D. Specific VPN Communities

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: