

156-215.80.302q

Number: 156-215.80

Passing Score: 800

Time Limit: 120 min

156-215.80



Website: <https://vceplus.com>

VCE to PDF Converter: <https://vceplus.com/vce-to-pdf/>

Facebook: <https://www.facebook.com/VCE.For.All.VN/>

Twitter : https://twitter.com/VCE_Plus

<https://vceplus.com/>

Check Point Certified Security Administrator R80

Exam A

QUESTION 1

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?



<https://vceplus.com/>

- 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 2

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 3

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 4

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or via CLI. Which command should he 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 <code>lock database override</code> and <code>unlock database</code> commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	<ul style="list-style-type: none">o <code>lock database override</code>o <code>unlock database</code>

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

QUESTION 5

Examine the following Rule Base.



Standard +

Access Control

- Policy
- NAT

Threat Prevention

- Policy
- Exceptions

Shared Policies

- Geo Policy

Access Tools

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

Summary Details Logs History

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

1.1.1.248

8 Draft change

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

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

Correct Answer: D

Section: (none)


Explanation

Explanation/Reference:

Explanation:

On top of the print screen there is a number "8" which consists for the number of changes made and not saved.

Session Management Toolbar (top of SmartConsole)

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

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

QUESTION 6

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

- A. The Gaia /bin/confd is locked by another administrator from a SmartConsole session.
- B. The database is locked by another administrator SSH session.
- C. The Network address of his computer is in the blocked hosts.



VMware R80-MGMT

View mode: Advanced

Network Management ▸ Hosts and DNS

System Name

Host Name:

Domain Name:

DNS

DNS Suffix:

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

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 7

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

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



Objects • Install Policy • Discard • Session: AppCtrl_and_DataAware • 39 • Publish

Standard x App-Policy-Layer x +

Access Control

- Policy
 - Network
 - AppCtrl
 - AppCtrl_DataAware
- NAT

Shared Policies

- Geo Policy
- Policy
- Gateways
- Exceptions

Related Tools

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

Search for IP, object, action, ...

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

Publish Error

Publish failed

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

Show pane

Summary Details

Drop Rule 1

Facebook

Created by: admin

Date created: Mar 01, 2016

Expiration time: Never

Hit Count: 0 (0%, Zero)

Policy installation - Standard Succeeded • 10.1.1.101

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.

To publish, you must fix the errors.

Reference:

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

QUESTION 8

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

QUESTION 10

To optimize Rule Base efficiency the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

It is logical that if lesser rules are checked for the matched rule to be found the lesser CPU cycles the device is using. Checkpoint match a session from the first rule on top till the last on the bottom.

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

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

QUESTION 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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation: **vpn**

tu

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

Usage vpn tu
vpn tunnelutil
Example vpn tu
Output



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

(1)          List all IKE SAs
(2)          List all IPsec SAs
(3)          List all IKE SAs for a given peer (GW) or user (Client)
(4)          List all IPsec SAs for a given peer (GW) or user (Client)
(5)          Delete all IPsec SAs for a given peer (GW)
(6)          Delete all IPsec SAs for a given User (Client)
(7)          Delete all IPsec+IKE SAs for a given peer (GW)
(8)          Delete all IPsec+IKE SAs for a given User (Client)
(9)          Delete all IPsec SAs for ALL peers and users
(0)          Delete all IPsec+IKE SAs for ALL peers and users

(Q)          Quit
```

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

QUESTION 21

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

- A. Security questions
- B. Check Point password

- C. SecurID
- D. RADIUS

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Authentication Schemes :- Check Point Password

- Operating System Password
- RADIUS
- SecurID
- TACAS

- Undefined If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

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

QUESTION 22

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To create a new permission profile:

1. In SmartConsole, go to **Manage & Settings > Permissions and Administrators > Permission Profiles**.
2. Click **New Profile**.

The **New Profile** window opens.

3. Enter a unique name for the profile.

4. Select a profile type:

- **Read/Write All** - Administrators can make changes

- **Auditor (Read Only All)** - Administrators can see information but cannot make changes ▪

Customized - [Configure custom settings](#)

5. Click **OK**.

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

QUESTION 23

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Packages and licenses are loaded into these repositories from several sources:

- the Download Center web site (packages)
- the Check Point DVD (packages) ▪ the User Center (licenses) ▪ by importing a file (packages and licenses) ▪ by running the `cplic` command line

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

QUESTION 24

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 25

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

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

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



layer and then after accepting the packet it passes to Threat Prevention layer.

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

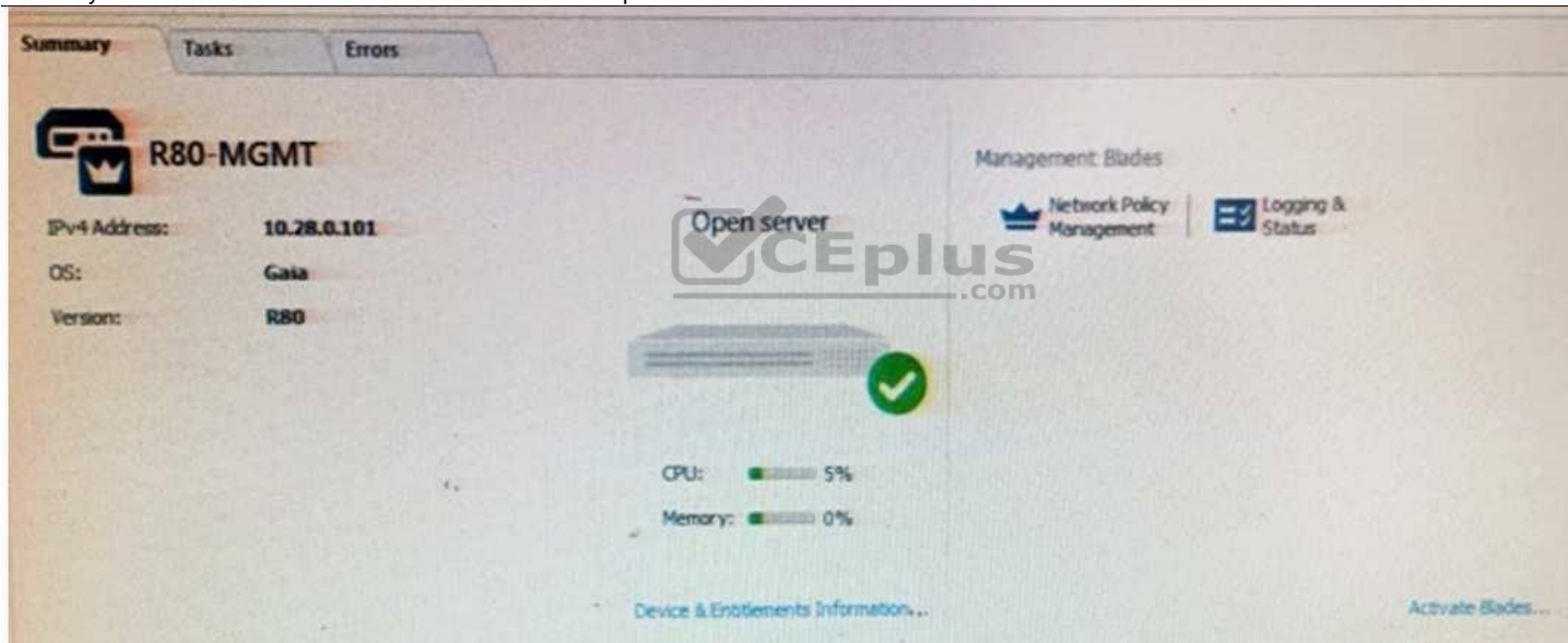
For example, when you upgrade to R80 from earlier versions:

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

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

QUESTION 26

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



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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Open Server	Non-Check Point hardware platform that is certified by Check Point as supporting Check Point products. Open Servers allow customers the flexibility of deploying Check Point software on systems which have not been pre-hardened or pre-installed (servers running standard versions of Solaris, Windows, Red Hat Linux).
--------------------	--

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

QUESTION 27

Choose what BEST describes the Policy Layer Traffic Inspection.

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.checkpoint.com/thread/1092>

QUESTION 28

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 29

What does the “unknown” SIC status shown on SmartConsole mean?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

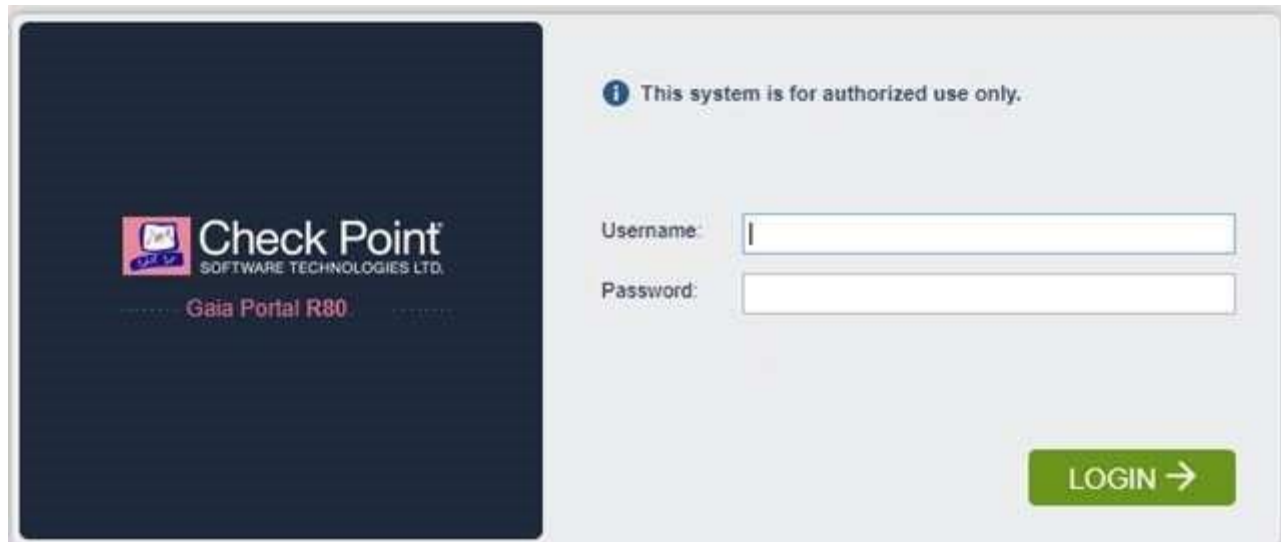
Explanation:

The most typical status is **Communicating**. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is **Unknown** then there is no connection between the Gateway and the Security Management server. If the SIC status is **Not Communicating**, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

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

QUESTION 30

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



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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

In Clish

A. Connect to command line on Security Gateway / *each* Cluster member.

B. Log in to Clish.

C. Set the desired port (e.g., port 4434):**HostName> set web ssl-port <Port_Number>** D. Save the changes:

HostName> save config

E. Verify that the configuration was saved:

[Expert@HostName]# grep 'httpd:ssl_port' /config/db/initial Reference:

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

QUESTION 31

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To enable Identity Awareness:

1. Log in to SmartDashboard.
2. From the Network Objects tree, expand the **Check Point** branch.
3. Double-click the Security Gateway on which to enable Identity Awareness.
4. In the Software Blades section, select **Identity Awareness** on the Network Security tab.

The **Identity Awareness** Configuration wizard opens.

5. Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

- **AD Query** - Lets the Security Gateway seamlessly identify Active Directory users and computers.
- **Browser-Based Authentication** - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

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

QUESTION 32

Which default user has full read/write access?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

The security Gateway is installed on GAI A 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 35

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 36

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 37

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 38

The following graphic shows:



Logs

New Tab

★ < > ↺ 🔍 Last 7 Days • src:10.1.1.202

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

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

- 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 39

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 40

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 41

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 42

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 43

Which application should you use to install a contract file?

- A. SmartView Monitor
- B. WebUI
- C. SmartUpdate
- D. SmartProvisioning

Correct Answer: C

Section: (none)

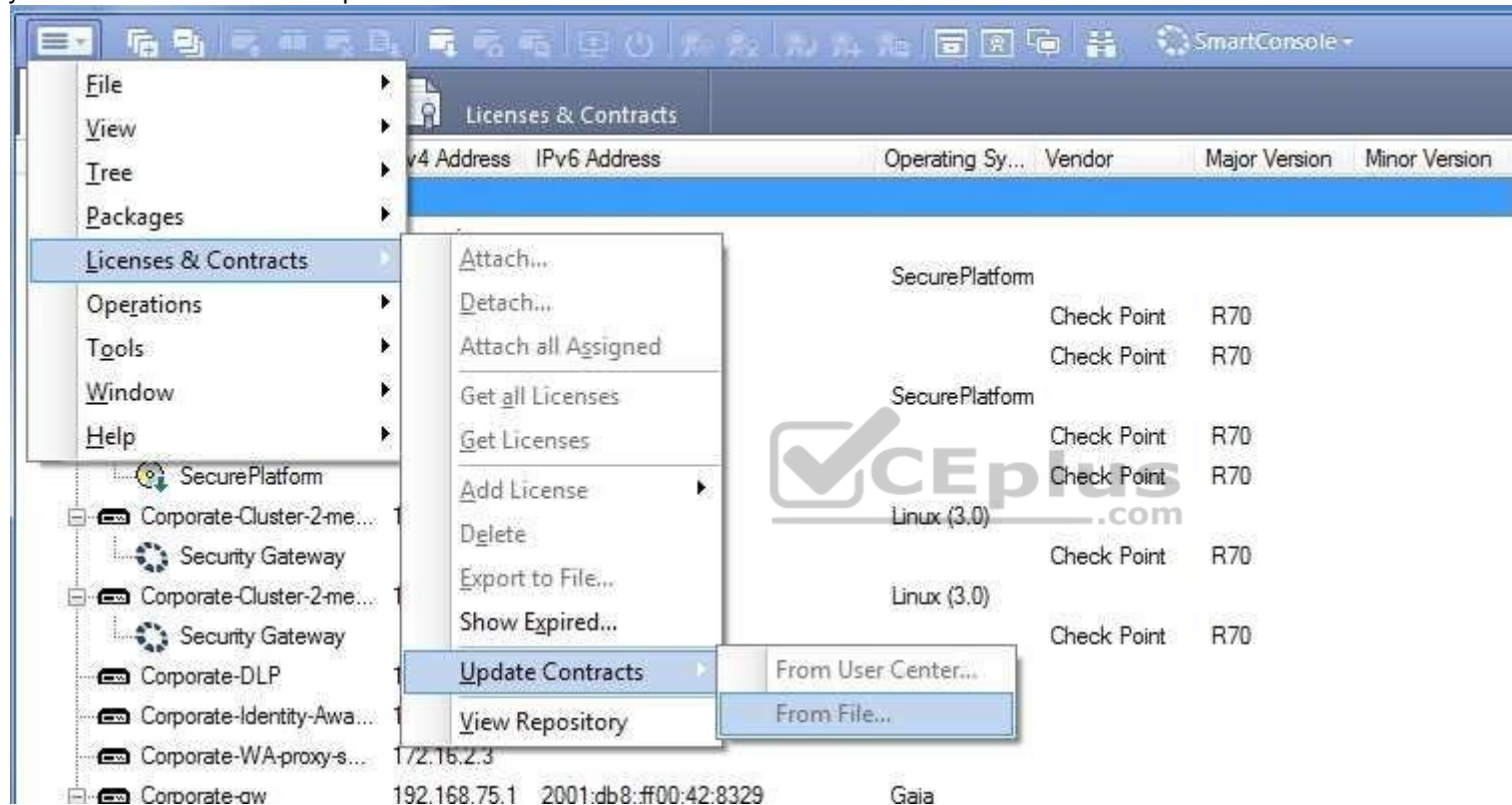
Explanation

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 44

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 45

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 46

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 47

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

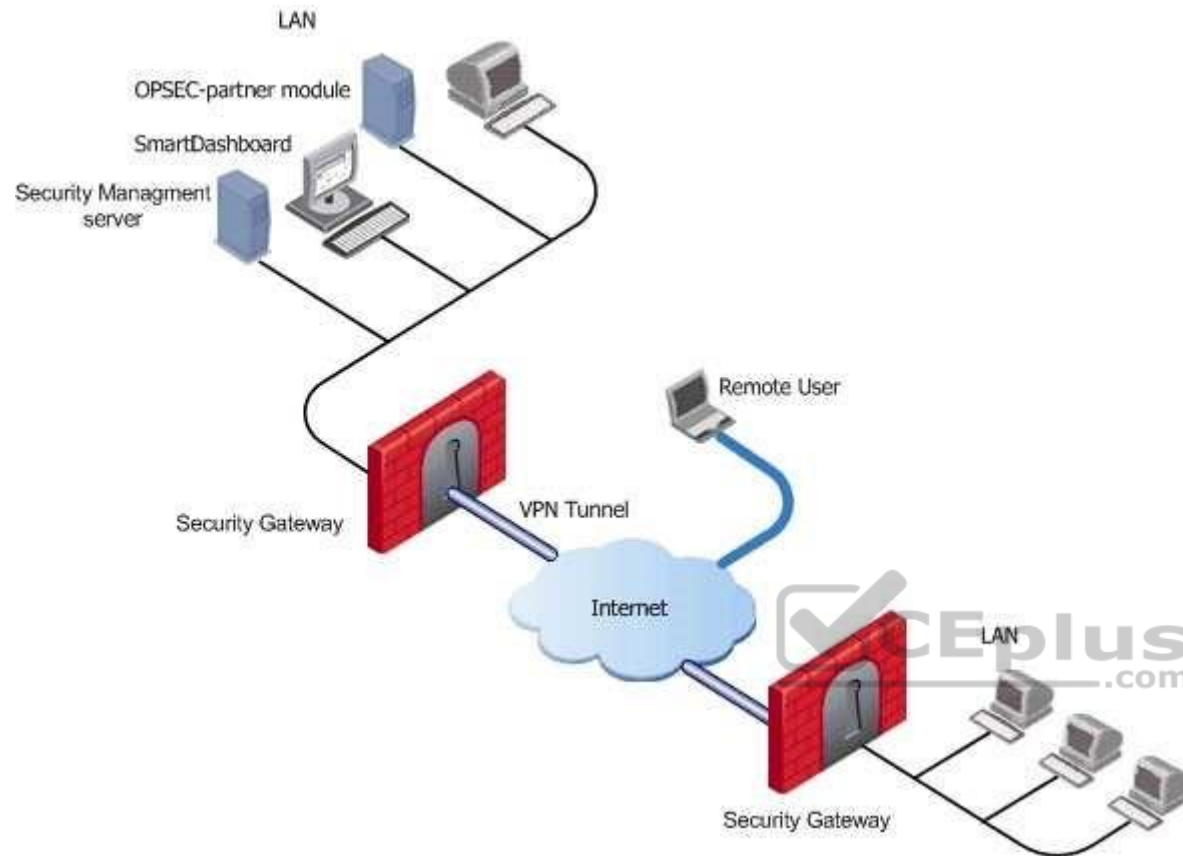
Explanation/Reference:

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 48

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 49

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?

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_indexer
SMARTLOG_SERVER	7977	E	1		[16:32:53] 5/5/2016	N	/opt/CPSmartLog-R80/smartlog_server
SVR	8045	E	1		[16:32:54] 5/5/2016	N	SVRServer
DASERVICE	8054	E	1		[16:32:54] 5/5/2016	N	DAService_script
CPSM	0	T	0		[17:17:02] 5/5/2016	N	cpstat_monitor

- 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.

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 50

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 51

Which of the following are types of VPN communicaties?

- 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 52

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 53

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 54

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 55

The Administrator wishes to update IPS protections from SmartConsole by clicking on the option “**Update Now**” under the Updates tab in Threat Tools. Which device requires internet access for the update to work?

- A. Security Gateway only
- B. Only the device where SmartConsole is installed
- C. Only the Security Management Server
- D. Either the Security Management Server or device where SmartConsole is installed

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 56

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 57

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 58

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 59

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 60

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 61

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 62

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 63

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 64

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 65

Which of the following licenses are considered temporary?

- A. Perpetual and Trial
- B. Plug-and-play and Evaluation



<https://vceplus.com/>



- 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 66

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 68

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

On the following picture an administrator configures Identity Awareness:



Check Point Gateway - A-GW

General Properties

- + Network Management
- + NAT
- HTTPS Inspection
- HTTP/HTTPS Proxy
- Anti-Bot and Anti-Virus
- Platform Portal
- UserCheck
- Mail
- IPS
- + VPN
- + Monitoring
- + Data
- + Monitoring
- + Log
- + Feeds
- + Options
- + Other

Machine

Name: Color:

IPv4 Address: ☐ Dynamic Address

IPv6 Address:

Identity Awareness Configuration

Methods For Acquiring Identity

Select how users will be identified by your security gateway.

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

ies:

After clicking “Next” the above configuration is supported by:

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

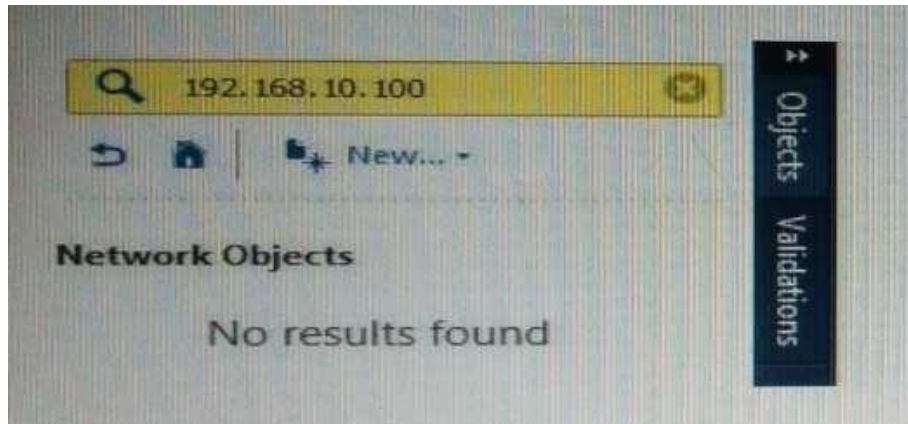
To enable Identity Awareness:

1. Log in to R80 SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Gateway on which to enable Identity Awareness.
3. On the Network Security tab, select **Identity Awareness**. The **Identity Awareness** Configuration wizard opens.
4. Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.
 - **AD Query** - Lets the Security Gateway seamlessly identify Active Directory users and computers.
 - **Browser-Based Authentication** - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.
 - **Terminal Servers** - Identify users in a Terminal Server environment (originating from one IP address).

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

QUESTION 70

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



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

Correct Answer: B

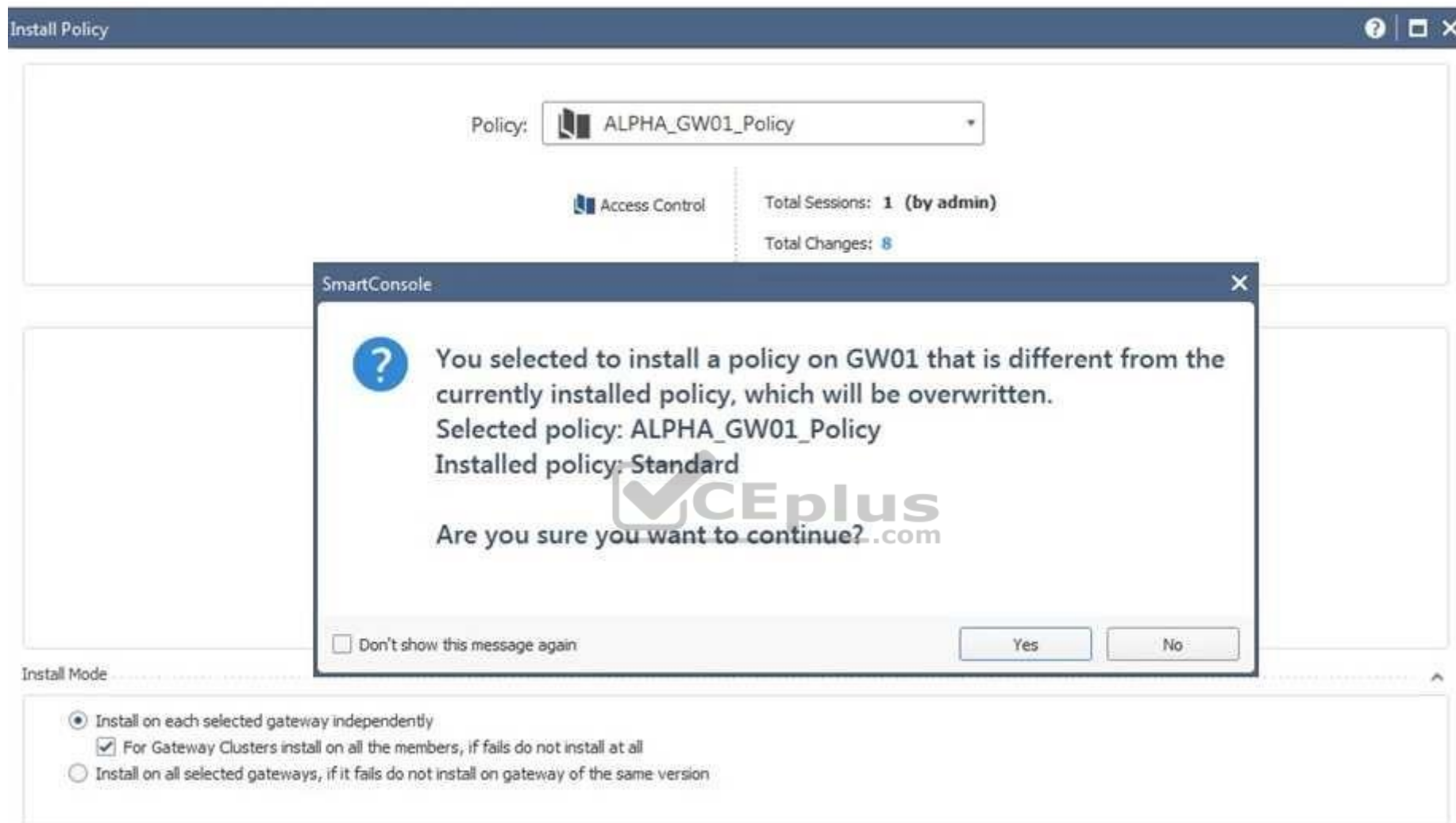
Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

Why would an administrator see the message below?



- A. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- D. A new Policy Package created on the Gateway and transferred to the Management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 73

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Introduction to the ICA

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

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

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

QUESTION 74

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

QUESTION 75

Fill in the blank: _____ information is included in the “Full Log” tracking option, but is not included in the “Log” tracking option?

- A. file attributes
- B. application
- C. destination port
- D. data type

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Tracking Options

- **Network Log** - Generates a log with only basic Firewall information: Source, Destination, Source Port, Destination Port, and Protocol.

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

None - Do not generate a log.

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

QUESTION 76

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 77

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

- A. Full
- B. Light
- C. Custom
- D. Complete

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 78

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

What Happens When a Security Gateway Recovers?

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

- Maintain Current Active Security Gateway means that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events.

- Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

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

QUESTION 80

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

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

QUESTION 81

In order to modify Security Policies the administrator can use which of the following tools?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Migrating from Traditional Mode to Simplified Mode

To migrate from Traditional Mode VPN to Simplified Mode:

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

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

Traditional or Simplified per new Firewall Policy

2. Click **OK**.

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

The **Manage Policies** window opens.

4. Click **New**.

The **New Policy** window opens.

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

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

Reference: http://dl3.checkpoint.com/paid/05/05e695b2012b4fd1d2bdfeccecd29290/CP_R80BC_VPN_AdminGuide.pdf?HashKey=1479823792_55fbc10656c87db4fcf742f4899ba90d&xtn=.pdf

QUESTION 83

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

- Software Blades

- Container

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

QUESTION 84

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Service Contract File

Following the activation of the license, a Service Contract File should be installed. This file contains important information about all subscriptions purchased for a specific device and is installed via SmartUpdate. A detailed explanation of the Service Contract File can be found in [sk33089](#). Reference:

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

QUESTION 85

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Check Point's QoS Solution

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

QUESTION 86

Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

- A. When Joe logs in, Bob will be log out automatically.
- B. Since they both are log in on different interfaces, they both will be able to make changes.
- C. If Joe tries to make changes, he won't, database will be locked.
- D. Bob will be prompt that Joe logged in.

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

QUESTION 87

Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as _____

- A. UserCheck
- B. User Directory
- C. User Administration
- D. User Center

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.

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

QUESTION 88

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 89

AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule?

- 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 90

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 91

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

- A. ISO 37001
- B. Sarbanes Oxley (SOX)
- C. HIPAA
- 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 92

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Obtaining a Configuration Lock

- lock database override
- unlock database

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

QUESTION 93

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 95

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

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

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This is the order that rules are enforced:

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

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

QUESTION 96

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 97

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

How RADIUS Accounting Works with Identity Awareness

RADIUS Accounting gets identity data from **RADIUS Accounting Requests** generated by the RADIUS accounting client.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/62050

QUESTION 98

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Event Analysis with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.

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

QUESTION 99

Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

- A. Firewall
- B. Identity Awareness
- C. Application Control
- D. URL Filtering

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.

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

QUESTION 100

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 102

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

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

To make this scenario work, the IT administrator:

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

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 104

MyCorp has the following NAT rules. You need to disable the NAT function when Alpha-internal networks try to reach the Google DNS (8.8.8.8) server. What can you do in this case?

- A. Use manual NAT rule to make an exception
- B. Use the NAT settings in the Global Properties
- C. Disable NAT inside the VPN community
- D. Use network exception in the Alpha-internal network object



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 105

What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

- A. degrades performance as the Security Policy grows in size
- B. requires additional Check Point appliances
- C. requires additional software subscription
- D. increases cost

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 106

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 107

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 108

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 109

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 110

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 111

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 112

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 113

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 114

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)

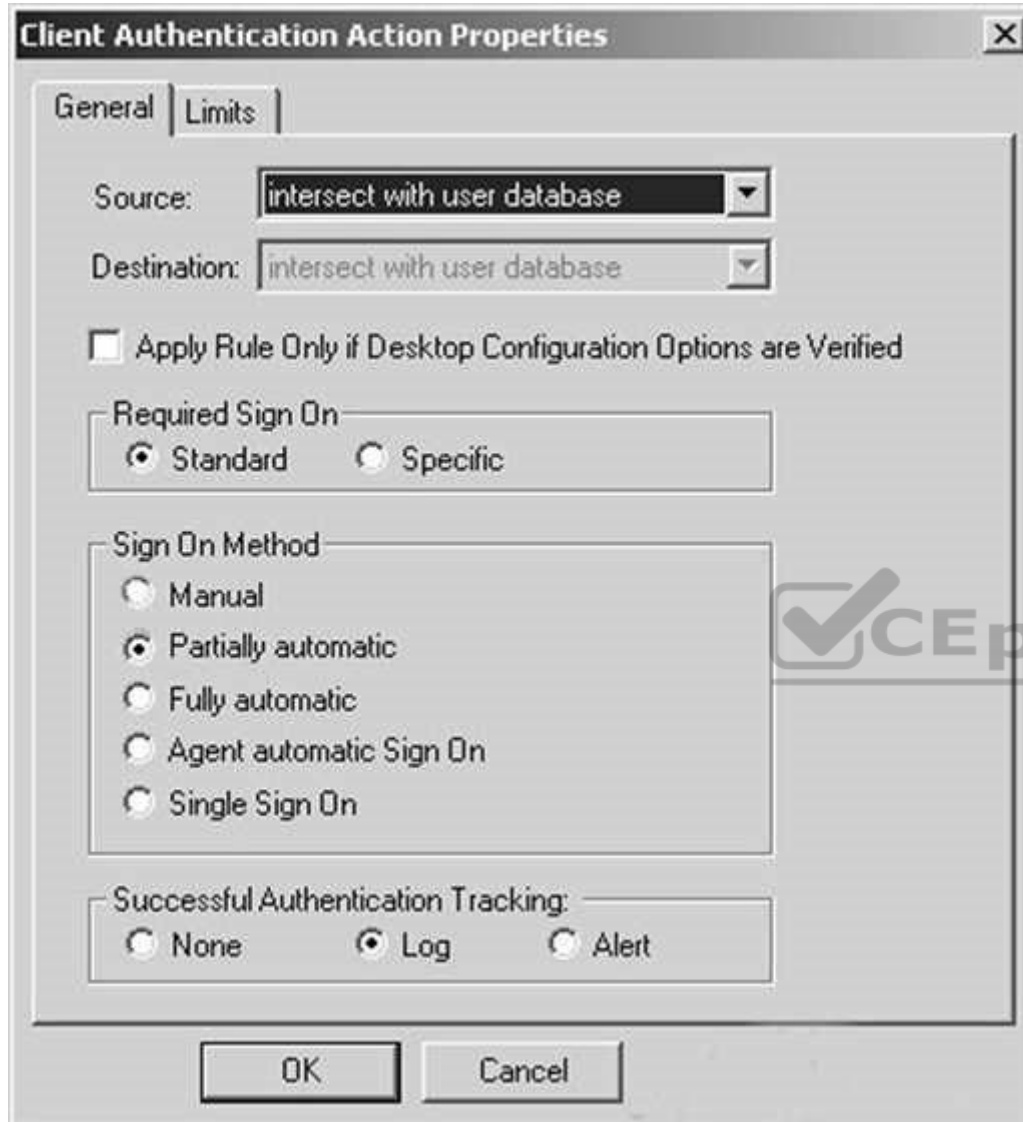
Explanation

Explanation/Reference:

QUESTION 115

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

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



Client Authentication Action Properties

General | Limits

Source: intersect with user database

Destination: intersect with user database

☐ Apply Rule Only if Desktop Configuration Options are Verified

Required Sign On

☒ Standard ☐ Specific

Sign On Method

☐ Manual

☒ Partially automatic

☐ Fully automatic

☐ Agent automatic Sign On

☐ Single Sign On

Successful Authentication Tracking:

☐ None ☒ Log ☐ Alert

OK Cancel

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 116

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 117

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 118

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 119

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 120

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 121

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 122

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 123

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 124

You want to establish a VPN, using certificates. Your VPN will exchange certificates with an external partner. Which of the following activities should 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 125

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 126

What is the appropriate default Gaia Portal address?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:**QUESTION 127**

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

**QUESTION 128**

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

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

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 129

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 130

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 131

A digital signature:

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 132

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

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 133

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 134

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 135

A Cleanup rule:

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 136

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 137

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 138

Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

- A. Check Point Password
- B. TACACSC. LDAP



<https://vceplus.com/> D.

Windows password

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 139

An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).

Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval.

If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute.

Which of the following is the BEST explanation for this behavior?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 140

Choose the correct statement regarding Implicit Rules.

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 141

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

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

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

- B. Run `fwm_dbexport` to export the user database. Select restore the entire database in the Database Revision screen. Then, run `fwm_dbimport`.
- C. Restore the entire database, except the user database, and then create the new user and user group.
- D. Restore the entire database, except the user database.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 143

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 144

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 145

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 146

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 147

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 148

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 149

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 150

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 151

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 152

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 153

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 154

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 155

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 156

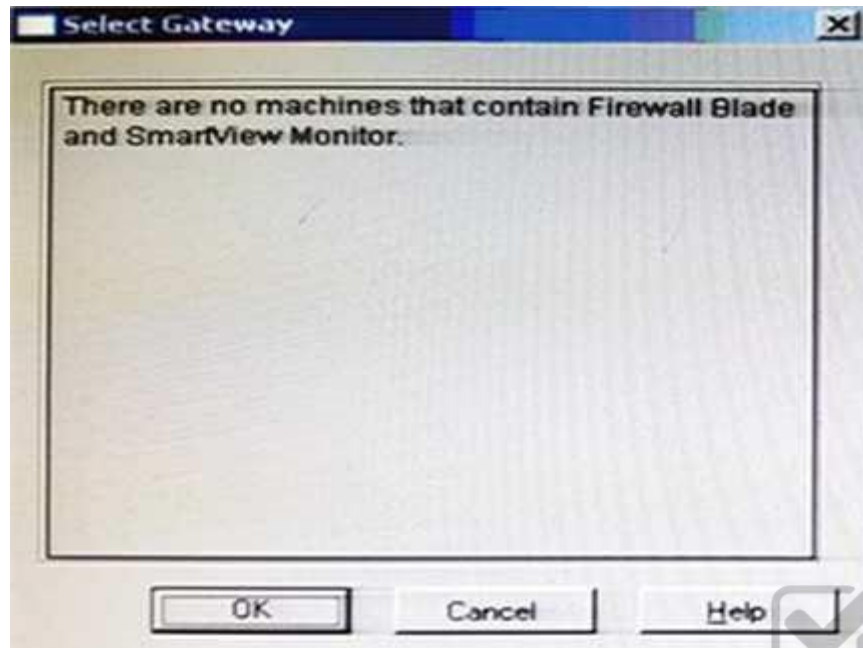
You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.



Unfortunately, you get the message:

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

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



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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157

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 suspicion?

- A. SmartDashboard
- B. SmartUpdate
- C. SmartView Status

D. SmartView Tracker

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

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 159

How do you configure the Security Policy to provide users 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 160

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, SMTP, 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 161

As a Security Administrator, you must refresh the Client Authentication authorized time-out every time a new user connection is authorized. How do you do this? Enable the **Refreshable Timeout** setting:

- A. in the user object's **Authentication** screen.
- B. in the Gateway object's **Authentication** screen.
- C. in the **Limit** tab of the **Client Authentication Action Properties** screen.
- D. in the **Global Properties Authentication** screen.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 162

When using GAIa, it might be necessary to temporarily change the MAC address of the interface `eth 0` to `00:0C:29:12:34:56`. After restarting the network the old MAC address should be active. How do you configure this change?

- A. As expert user, issue these commands:

```
# IP link set eth0 down
# IP link set eth0 addr 00:0C:29:12:34:56
# IP link set eth0 up
```
- B. Edit the file `/etc/sysconfig/netconf.C` and put the new MAC address in the field

```
(conf
: (conns
```

```
: (conn
:hwaddr ("00:0C:29:12:34:56")
```

C. As expert user, issue the command:

```
# IP link set eth0 addr 00:0C:29:12:34:56
```

D. Open the WebUI, select **Network > Connections > eth0**. Place the new MAC address in the field **Physical Address**, and press **Apply** to save the settings.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 163

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

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his desktop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location. 3) Changes from static IP address to DHCP for the client PC.

What should John request when he cannot access the web server from his laptop?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 164

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

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

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 165

Which component functions as the Internal Certificate Authority for R77?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 166

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

- A. Create new dashboards to manage 3rd party task

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 167

In what way are SSL VPN and IPSec VPN different?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 168

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 169

Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 170

To fully enable Dynamic Dispatcher on a Security Gateway:

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 171

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 172

What is the purpose of Priority Delta in VRRP?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 173

The Firewall kernel is replicated multiple times, therefore:

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 174

There are 4 ways to use the Management API for creating host object with R80 Management API. Which one is NOT correct?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 175

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

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 176

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 177

Which remote Access Solution is clientless?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 178

What component of R80 Management is used for indexing?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 179

Which NAT rules are prioritized first?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 180

What is the difference between an event and a log?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 181

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 182

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 183

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 184

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 185

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 186

Using ClusterXL, what statement is true about the Sticky Decision Function?

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



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 187

What command would show the API server status?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 188

How Capsule Connect and Capsule Workspace differ?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 189

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

- A. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- C. Time object to a rule to make the rule active only during specified times.
- D. Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 190

What are the three components for Check Point Capsule?

- A. Capsule Docs, Capsule Cloud, Capsule Connect
- B. Capsule Workspace, Capsule Cloud, Capsule Connect
- 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 191

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265
- B. TCP port 265
- C. UDP port 256
- D. TCP port 256

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 192

What is true about the IPS-Blade?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 193

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

- A. Go to clash-Run cpstop | Run cpstart
- B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
- C. Administrator does not need to perform any task. Check Point will make use of the newly installed CPU and Cores
- D. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 194

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

- A. Any size
- B. Less than 20GB
- C. More than 10GB and less than 20 GB
- D. At least 20GB

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 195

Which firewall daemon is responsible for the FW CLI commands?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 196

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 197

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 198

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the “mgmt_cli” command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia’s secure shell (clash)19+
- D. Sending API commands over an http connection using web-services

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 199

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

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 200

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 201

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 202

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 203

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 204

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 205

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 206

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 207

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

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



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 208

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 209

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 210

What are the steps to configure the HTTPS Inspection Policy?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 211

What is the difference between SSL VPN and IPSec VPN?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 212

Which statement is NOT TRUE about Delta synchronization?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 213

Under which file is the proxy arp configuration stored?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 214

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 215

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

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 216

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

- A. secondary Smartcenter
- B. active Smartcenter



<https://vceplus.com/>

- C. connect virtual IP of Smartcenter HA
- D. primary Smartcenter

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 217

Which path below is available only when CoreXL is enabled?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 218

Which of the following describes how Threat Extraction functions?

- A. Detect threats and provides a detailed report of discovered threats
- B. Proactively detects threats

- C. Delivers file with original content
- D. Delivers PDF versions of original files with active content removed

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 219

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 220

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 221

What SmartEvent component creates events?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 222

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 223

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 224

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:



QUESTION 225

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 226

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 227

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 228

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 229

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 230

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 231

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 232

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 233

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 234

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 235

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 236

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 237

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 238

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 239

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 240

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 241

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 242

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 243

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 244

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 245

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 246

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 247

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 248

Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

- A. AES-GCM-256
- B. AES-CBC-256
- C. AES-GCM-128
- D. DES

Correct Answer: B

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/13847

QUESTION 249

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

- A. DLP shared policy
- B. Geo policy shared policy
- C. Mobile Access software blade
- D. HTTPS inspection

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Shared Policies

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

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

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

QUESTION 250

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 251

Consider the Global Properties following settings:

Global Properties

- + FireWall-1
 - NAT - Network Address
 - Authentication
- + VPN
 - Identity Awareness
 - UTM-1-Edge Gatew
- + Remote Access
 - User Directory
 - QoS
 - User Authority
 - User Accounts
 - ConnectControl
 - Stateful Inspection
- + Log and Alert
 - OPSEC
 - Security Managemer
 - Non Unique IP Addr
 - Proxy
 - IPS
 - UserCheck
 - Hit Count
 - Advanced

Select the following properties and choose the position of the rules in the Rule Base:

- ☒ Accept control connections: First
- ☒ Accept Remote Access control connections: First
- ☒ Accept Smart Update connections: First
- ☒ Accept IPS-1 management connections: First
- ☒ Accept outgoing packets originating from Gateway: Before Last
- ☒ Accept outgoing packets originating from Connections gateway: Before Last
- ☐ Accept RIP: First
- ☒ Accept Domain Name over UDP (Queries): First
- ☐ Accept Domain Name over TCP (Zone Transfer): First
- ☐ Accept ICMP requests: Before Last
- ☒ Accept Web and SSH connections for Gateway's administration (Small Office Appliance): First
- ☒ Accept incoming traffic to DHCP and DNS services of gateways (Small Office Appliance): First
- ☒ Accept Dynamic Address modules' outgoing Internet connections: First
- ☒ Accept VRRP packets originating from cluster members (VSX IPSO VRRP): First
- ☒ Accept Identity Awareness control connections: First

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 252

How is communication between different Check Point components secured in R80?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 253

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

- A. 259, 900
- B. 256, 257
- C. 8080, 529
- D. 80, 256

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 254

What is the purpose of the CPCA process?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 255

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

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

Create new user with any UID and assign role to the user.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 256

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 257

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 258

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

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

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

QUESTION 259

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 260

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 261

What is the purpose of a Clean-up Rule?

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



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

These are basic access control rules we recommend for all Rule Bases:

- Stealth rule that prevents direct access to the Security Gateway.
- Cleanup rule that drops all traffic that is not allowed by the earlier rules.

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

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm **QUESTION 262**

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:

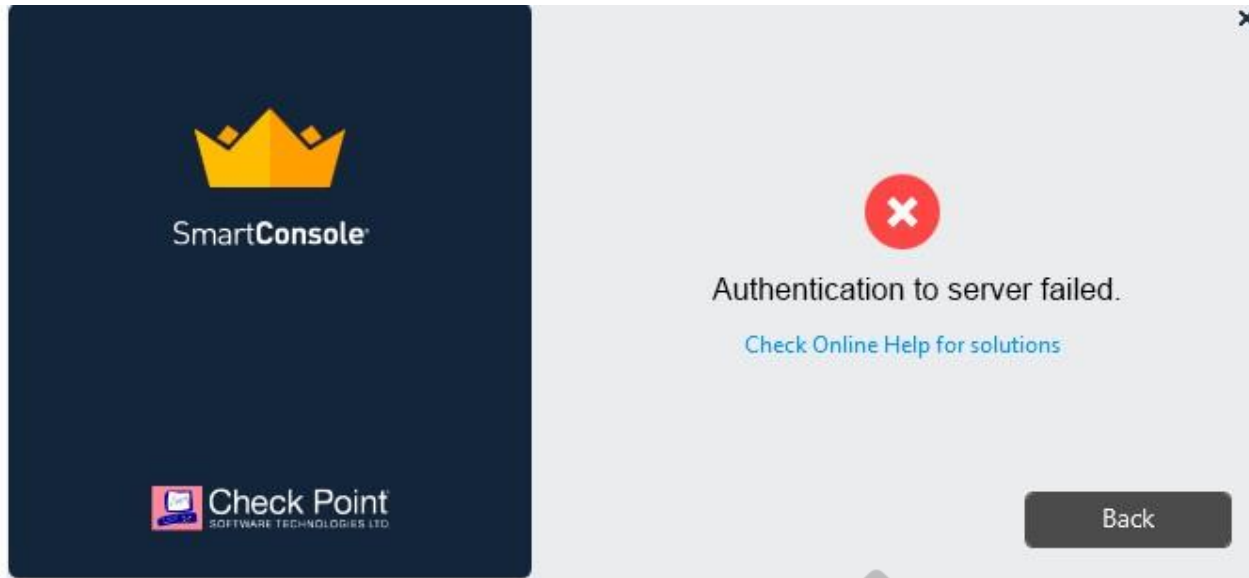
- **Static NAT** - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.
- **Hide NAT** - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the 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 263

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



What is the most likely reason?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 264

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

- A. The Global one also saves and publishes 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-selects the installation for only the current policy and for the applicable gateways.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 265

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

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

Correct Answer: C

Section: (none)

Explanation



Explanation/Reference:

Explanation:

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

Reference:

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

QUESTION 266

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 267

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 268

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 269

Which icon indicates in the WebUI that read/write access is enabled?

- A. Pencil
- B. Padlock
- C. Book
- D. Eyeglasses

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 270

What is NOT an advantage of Stateful Inspection?

- A. High Performance

- B. Good Security
- C. No Screening above Network layer
- D. Transparency

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 271

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 272

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:



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

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

Reference:

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

QUESTION 273

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 274

Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Anti-Bot

The Need for Anti-Bot

There are two emerging trends in today's threat landscape:

- A profit-driven cybercrime industry that uses different tools to meet its goals. This industry includes cyber-criminals, malware operators, tool providers, coders, and affiliate programs. Their "products" can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and denial of service attacks) and organizations are finding it difficult to fight off these attacks.
- Ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.

Both of these trends are driven by bot attacks.

A *bot* is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_ThreatPrevention_WebAdmin/102176.htm

QUESTION 275

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation: Configure **Spoof Tracking** - select the tracking action that is done when spoofed packets are detected: ▪

Log - Create a log entry (default)

- **Alert** - Show an alert
- **None** - Do not log or alert

Reference:

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

QUESTION 276

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To create an access role:

1. Select **Users and Administrators** in the Objects Tree.

2. Right-click **Access Roles > New Access Role**.
The **Access Role** window opens.

3. Enter a **Name** and **Comment** (optional) for the access role.

4. In the **Networks** tab, select one of these: ▪ **Any network**

▪ **Specific networks** - Click the plus sign and select a network.

Your selection is shown in the **Networks** node in the **Role Preview** pane.

5. In the **Users** tab, select one of these: ▪ **Any user**

▪ **All identified users** - Includes users identified by a supported authentication method (internal users, AD users or LDAP users). ▪
Specific users - Click the plus sign.

A window opens. You can search for Active Directory entries or select them from the list.

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

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

Specific machines - Click the plus sign.

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

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

8. Click **OK**.

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

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

QUESTION 277

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The first rule is the automatic rule for the **Accept All Encrypted Traffic** feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.

2. **Site to site VPN** - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.

3. **Remote access** - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

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

QUESTION 278

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 279

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 280

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 281

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

- A. Both User and Objects databases
- B. Network databases only
- C. Objects databases only
- D. User databases only

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 282

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 283

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 284

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 (*/v_current*) disk partition. This includes Check Point products, configuration, and operating system. Starting in **R77.10**, exporting an image from one machine and importing that image on another machine of the same type is supported. The *log* partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be saved.

Reference:

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

QUESTION 285

What is the purpose of the Stealth Rule?

- A. To prevent users from directly connecting to a Security Gateway.
- B. To reduce the number of rules in the database.
- C. To reduce the amount of logs for performance issues.
- D. To hide the gateway from the Internet.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <http://www.pearsonitcertification.com/articles/article.aspx?p=387728&seqNum=3>

QUESTION 286

What key is used to save the current CPView page in a filename format cpview_“cpview process ID”. cap”number of captures”?

- A. S
- B. W
- C. C
- D. Space bar



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_SecurityManagement_AdminGuide/html_frameset.htm?topic=documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_SecurityManagement_AdminGuide/204685

QUESTION 287

Fill in the blank: It is Best Practice to have a _____ rule at the end of each policy layer.

- A. Explicit Drop
- B. Implied Drop
- C. Explicit CleanUp
- D. Implicit Drop

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_SmartDashboard_OLH/html_frameset.htm?topic=documents/R80/CP_R80_SmartDashboard_OLH/NFHf4E9NLQBJIVkHRpc16w2

QUESTION 288

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 289

Fill in the blank: Once a certificate is revoked from the Security GateWay by the Security Management Server, the certificate information is _____.

- A. Sent to the Internal Certificate Authority.
- B. Sent to the Security Administrator.
- C. Stored on the Security Management Server.
- D. Stored on the Certificate Revocation List.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 290

Which type of attack can a firewall NOT prevent?

- A. Network Bandwidth Saturation
- B. Buffer Overflow
- C. SYN Flood
- D. SQL Injection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 291

R80 is supported by which of the following operating systems:

- A. Windows only
- B. Gaia only
- C. Gaia, SecurePlatform, and Windows
- D. SecurePlatform only

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://community.checkpoint.com/t5/General-Management-Topics/R80-x-FAQ/td-p/39994>

QUESTION 292

What Check Point technologies deny or permit network traffic?

- A. Application Control, DLP
- B. Packet Filtering, Stateful Inspection, Application Layer Firewall.
- C. ACL, SandBlast, MPT
- D. IPS, Mobile Threat Protection

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:



QUESTION 293

What licensing feature is used to verify licenses and activate new licenses added to the License and Contracts repository?

- A. Verification tool
- B. Verification licensing
- C. Automatic licensing
- D. Automatic licensing and Verification tool

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 294

The “Hit count” feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits even if the Track option is set to “None”?

- A. No, it will not work independently. Hit Count will be shown only for rules with Track options set as Log or alert
- B. Yes, it will work independently as long as “analyze all rules” tick box is enabled on the Security Gateway
- C. No, it will not work independently because hit count requires all rules to be logged
- D. Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways

Correct Answer: D

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 295

To view the policy installation history for each gateway, which tool would an administrator use?

- A. Revisions
- B. Gateway installations
- C. Installation history
- D. Gateway history

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/119225

QUESTION 296

Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 297

Which of the following is NOT a valid deployment option for R80?

- A. All-in-one (stand-alone)
- B. Log server
- C. SmartEvent
- D. Multi-domain management server

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 298

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

- A. Right click Accept in the rule, select “More”, and then check “Enable Identity Captive Portal”
- B. On the firewall object, Legacy Authentication screen, check “Enable Identity Captive Portal”
- C. In the Captive Portal screen of Global Properties, check “Enable Identity Captive Portal”
- D. On the Security Management Server object, check the box “Identity Logging”

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 299

Which option will match a connection regardless of its association with a VPN community?

- 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:

QUESTION 300

What is a role of Publishing?

- A. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public
- B. The Security Management Server installs the updated policy and the entire database on Security Gateways

- C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways
- D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base

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/119225

QUESTION 301

Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

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

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

QUESTION 302

Which option in a firewall rule would only match and allow traffic to VPN gateways for one Community in common?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



<https://vceplus.com/>

