

156-215.80

Number: 156-215.80

Passing Score: 800

Time Limit: 120 min

File Version: 1

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/>

Exam A

QUESTION 1

Which of the following is NOT a SecureXL traffic flow?



<https://vceplus.com/>

- A. Medium Path
- B. Accelerated Path
- C. High Priority Path
- D. Slow Path



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:

Slow path - Packets and connections that are inspected by the Firewall and are not processed by SecureXL.

Accelerated path - Packets and connections that are offloaded to SecureXL and are not processed by the Firewall.

Medium path - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

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

QUESTION 2

VPN gateways authenticate using _____ and _____ .

- A. Passwords; tokens
- B. Certificates; pre-shared secrets
- C. Certificates; passwords
- D. Tokens; pre-shared secrets

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/85469.htm

QUESTION 3

Which of the following statements is TRUE about R80 management plug-ins?

- A. The plug-in is a package installed on the Security Gateway.
- B. Installing a management plug-in requires a Snapshot, just like any upgrade process.
- C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
- D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

You are the senior Firewall administrator for ABC Corp., and have recently returned from a training course on Check Point's new advanced R80 management platform. You are presenting an in-house overview of the new features of Check Point R80 Management to the other administrators in ABC Corp.



How will you describe the new “Publish” button in R80 Management Console?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

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

QUESTION 5

With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 6

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

- A. Logging has disk space issues. Change logging storage options on the logging server or Security Management Server properties and install database.
- B. Content Awareness is not enabled.
- C. Identity Awareness is not enabled.
- D. Log Trimming is enabled.

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 7

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 8

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server Operating System. He can do this via WebUI or via CLI. Which command should he use in CLI?

- 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 9

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 10

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 11

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 12

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

When you select **Install Policy**, you are prompted to publish all unpublished changes. You cannot install a policy if the included changes are not published.

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

QUESTION 13

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

- **License & Contract Repository**, which is stored on all platforms in the directory `$FWDIR\conf\`.

Package Repository, which is stored:

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

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

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

QUESTION 14

Using the SmartConsole, 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:

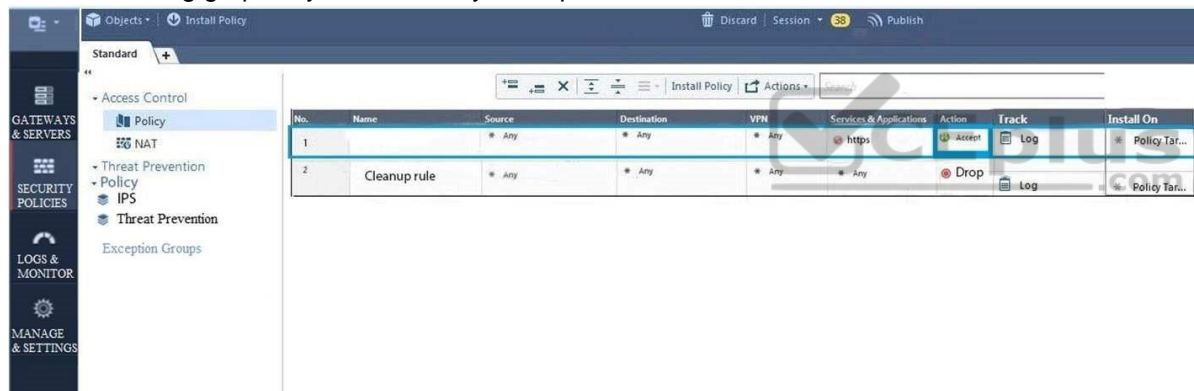
- **Read/Write All** - Administrators can make changes
- **Auditor (Read Only All)** - Administrators can see information but cannot make changes
- **Customized** - [Configure custom settings](#)

5. Click **OK**.

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

QUESTION 15

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 if it is accepted 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.

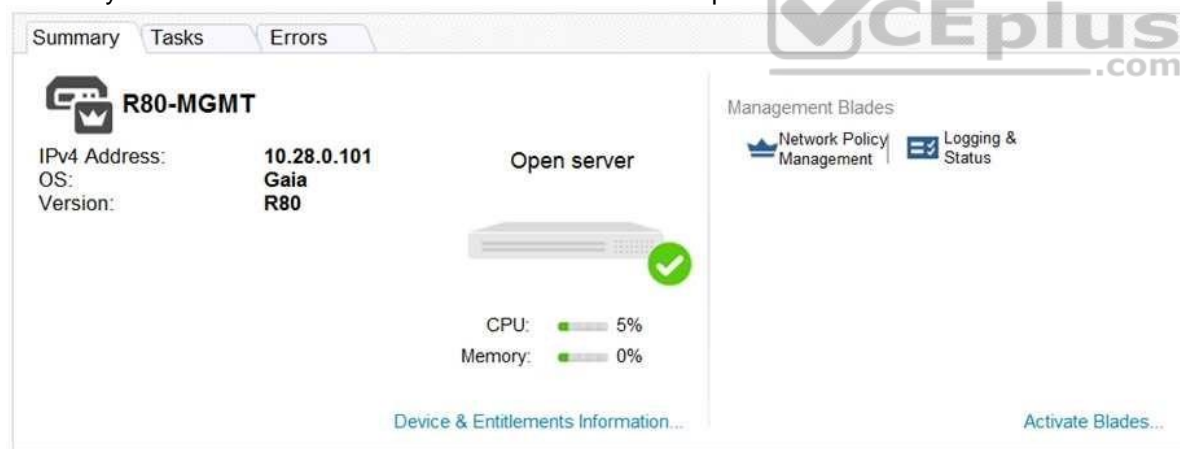
- Gateways that have the IPS and Threat Emulation Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention.

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 16

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.

D. A Check Point Management Server software using the Open SSL.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

QUESTION 17

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 18

The security Gateway is installed on GAIa R80. The default port for the WEB User Interface is _____ .

- A. TCP 18211
- B. TCP 257
- C. TCP 4433
- D. TCP 443

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

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 20

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 securityD. SandBlast



<https://vceplus.com/>

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 21

The R80 utility fw monitor is used to troubleshoot _____

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues
- D. Phase two key negotiation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

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

QUESTION 22

The R80 feature _____ permits blocking specific IP addresses for a specified time period.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an **Install Policy** operation

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartViewMonitor_AdminGuide/17670.htm

QUESTION 23

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

To enable Identity Awareness:

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

The **Identity Awareness** Configuration wizard opens.

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

- **AD Query** - Lets the Security Gateway seamlessly identify Active Directory users and computers.
- **Browser-Based Authentication** - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.
- **Terminal Servers** - Identify users in a Terminal Server environment (originating from one IP address). See

[Choosing Identity Sources](#).

Note - When you enable Browser-Based Authentication on a Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.

6. Click **Next**.

The Integration With Active Directory window opens.

When SmartDashboard is part of the domain, SmartDashboard suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with **all** of the domain controllers in the organization's Active Directory.

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

QUESTION 24

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Configuring Roles - CLI (rba)

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

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

QUESTION 25

What is NOT an advantage of Packet Filtering?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Packet Filter Advantages and Disadvantages

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

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

QUESTION 26

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

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

- A. a routing table
- B. that each Security Gateway enforces at least one rule
- C. a Demilitarized Zone
- D. a Security Policy install

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 28

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 29

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 30

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 31

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 32

In a Network policy with Inline layers, 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

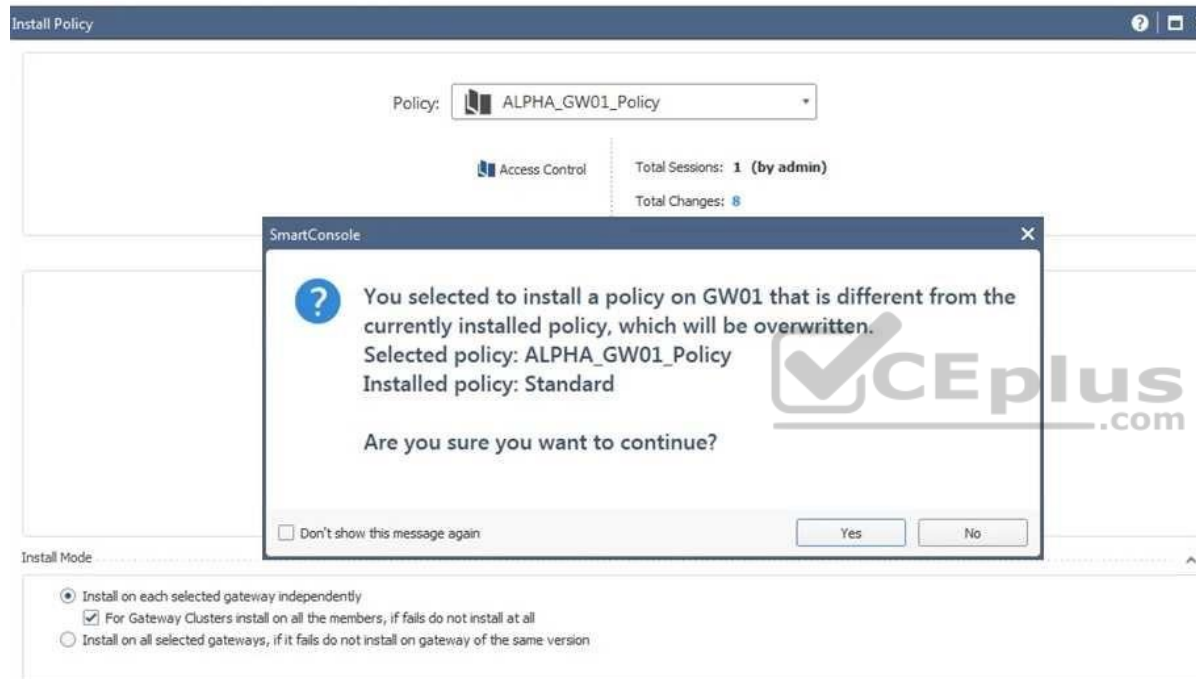
Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

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 34

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 35

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 logged out automatically.
- B. Since they both are logged in on different interfaces, they both will be able to make changes.
- C. The database will be locked by Bob and Joe will not be able to make any changes.
- D. Bob will receive a prompt that Joe logged in.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

Look at the following screenshot and select the BEST answer.



8	Customers to ftp servers	ExternalZone	FTP_Ext	* Any	ftp	Any Direction	Accept
---	--------------------------	--------------	---------	-------	-----	---------------	--------

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

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

- A. Log Implied Rule was not selected on Global Properties.
- B. Log Implied Rule was not set correctly on the track column on the rules base.

- C. Track log column is set to none.
- D. Track log column is set to Log instead of Full Log.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Implied Rules are configured only on Global Properties.

QUESTION 38

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

R80 can be installed only on GAIA OS.

Supported Check Point Installations All R80 servers are supported on the Gaia Operating System:

- Security Management Server
- Multi-Domain Security Management Server
- Log Server
- Multi-Domain Log Server
- SmartEvent Server

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

QUESTION 39



The IT Management team is interested in the new features of the Check Point R80.x Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80.x because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

- A. R80.x Management contains compatibility packages for managing earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- B. R80.x Management requires the separate installation of compatibility hotfix packages for managing the earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- C. R80.x Management was designed as a completely different Management system and so can only monitor Check Point Gateways prior to R80.
- D. R80.x Management cannot manage earlier versions of Check Point Gateways prior to R80. Only R80 and above Gateways can be managed. Consult the R80 Release Notes for more information.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Compatibility with Gateways



R80 Management Servers can manage gateways of these versions:

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

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

QUESTION 40

A _____ is used by a VPN gateway to send traffic as if it was a physical interface.

- A. VPN Tunnel Interface
- B. VPN community
- C. VPN router
- D. VPN interface

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Route Based VPN

VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it was a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols.

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

QUESTION 41

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 42

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 43

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 44

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 45

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 46

What action can be performed from SmartUpdate R77?

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:



QUESTION 48

Which directory holds the SmartLog index files by default?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

What statement is true regarding Visitor Mode?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

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 52

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_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 53

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 54

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 55

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 56

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 57

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 58

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

- A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
- B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
- C. SmartView Tracker, CPINFO, SmartUpdate
- D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

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

- A. From the Internet
- B. Through internal interfaces
- C. Through all interfaces
- D. According to the Firewall Policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:



QUESTION 61

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 62

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 63

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 64

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 65

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 66

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

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 68

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 69

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 70

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 71

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 72

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 73

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 74

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 75

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 76

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

- A. Install appliance TE250X on SpanPort on LAN switch in MTA mode
- B. Install appliance TE250X in standalone mode and setup MTA
- C. You can utilize only Check Point Cloud Services for this scenario

D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

[HashKey=1517091196_a292abdde351bbdb4b3d28e82654b240&xtn=.pdf](http://dl3.checkpoint.com/paid/f2/f2faf02dba06acad8cc4c57833593df6/CP_TE100X_TE250X_Appliance_GettingStartedGuide.pdf?HashKey=1517091196_a292abdde351bbdb4b3d28e82654b240&xtn=.pdf)

QUESTION 77

What is the mechanism behind Threat Extraction?

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



<https://vceplus.com/>

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

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 79

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 80

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 81

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 82

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 83

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 84

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 85

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

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 87

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 88

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 89

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 90

What protocol is specifically used for clustered environments?

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 91

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 92

Which message indicates IKE Phase 2 has completed successfully?

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 93**

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 94

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 95

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 96

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 97

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 98

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:**QUESTION 99**

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

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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 100

Which one of the following is TRUE?

- A. Ordered policy is a sub-policy within another policy
- B. One policy can be either inline or ordered, but not both

- C. Inline layer can be defined as a rule action
- D. Pre-R80 Gateways do not support ordered layers

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

Which of the following are types of VPN communities?

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

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

QUESTION 102

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network
- B. Network and Threat Prevention
- C. Application Control and URL Filtering
- D. Network and Application Control

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

The position of an implied rule is manipulated in the _____ window.

- A. NAT
- B. Firewall
- C. Global Properties
- D. Object Explorer

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 104

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 105

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 106

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 107

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 108

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 109

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 110

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 111

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

- A. Status monitoring
- B. Policy configuration
- C. Certificate authority
- D. Address translation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Reference:

www.checkfirewalls.com/datasheets/smartcenter_datasheet.pdf

QUESTION 112

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

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

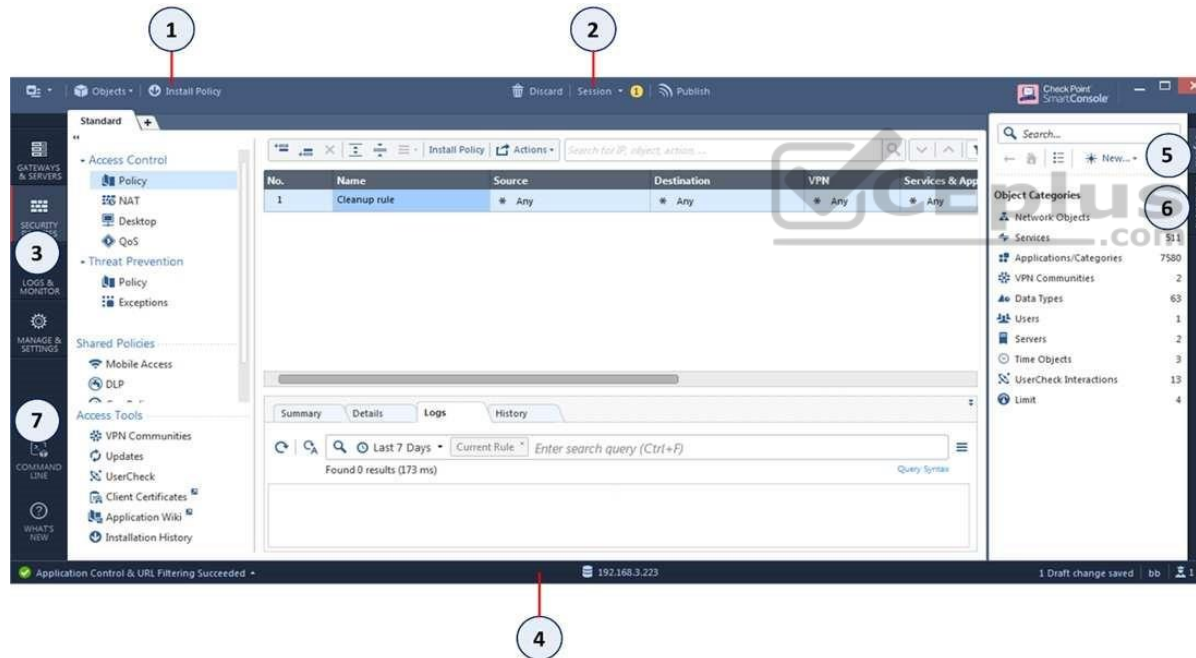
Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:



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

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

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

QUESTION 113

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

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Using Endpoint Identity Agents give you: ▪

User and machine identity

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

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

QUESTION 114

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 115

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 116

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 117

Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 118

When defining group-based access in an LDAP environment with Identity Awareness, what is the BEST object type to represent an LDAP group in a Security Policy?

- A. Access Role
- B. User Group
- C. SmartDirectory Group
- D. Group Template

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 119

How do you manage Gaia?

- A. Through CLI and WebUI
- B. Through CLI only
- C. Through SmartDashboard only
- D. Through CLI, WebUI, and SmartDashboard

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 120

An Endpoint identity agent uses a _____ for user authentication.

- A. Shared secret
- B. Token
- C. Username/password or Kerberos Ticket
- D. Certificate



Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 121

What is the purpose of a Stealth Rule?

- A. A rule used to hide a server's IP address from the outside world.
- B. A rule that allows administrators to access SmartDashboard from any device.
- C. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.
- D. A rule at the end of your policy to drop any traffic that is not explicitly allowed.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 122

Where is the “Hit Count” feature enabled or disabled in SmartConsole?

- A. On the Policy Package
- B. On each Security Gateway
- C. On the Policy layer
- D. In Global Properties for the Security Management Server

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/126197

QUESTION 123

Each cluster, at a minimum, should have at least _____ interfaces.

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

Correct Answer: C

Section: (none)

Explanation

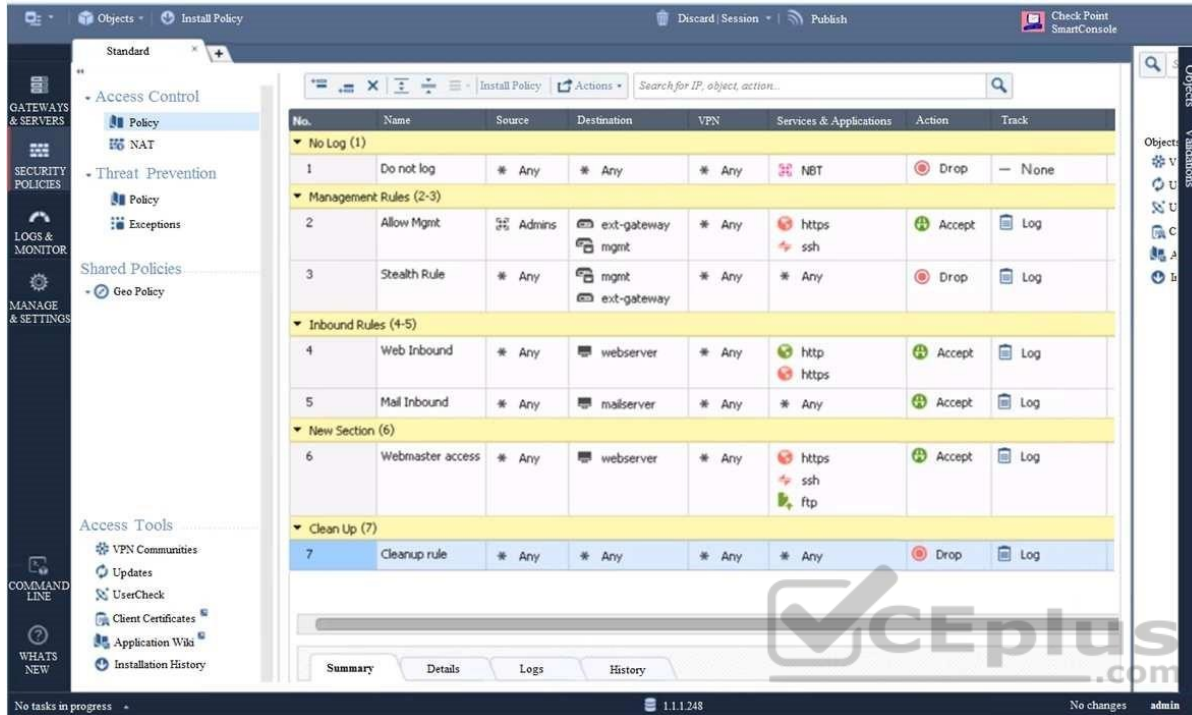
Explanation/Reference:

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

QUESTION 124

Examine the sample Rule Base.





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

What will be the result of a verification of the policy from SmartConsole?

- A. No errors or Warnings
- B. Verification Error: Empty Source-List and Service-List in Rule 5 (Mail Inbound)
- C. Verification Error: Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)
- D. Verification Error: Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 125

You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

- A. Open SmartLog and connect remotely to the wireless controller
- B. Open SmartEvent to see why they are being blocked
- C. Open SmartDashboard and review the logs tab
- D. Open SmartLog and filter for the IP address of the tablet

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 126

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

- A. RADIUS
- B. Remote Access and RADIUS
- C. All of the above
- 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 127

Which repositories are installed on the Security Management Server by SmartUpdate?

- A. License and Update
- B. Package Repository and Licenses
- C. Update and License & Contract
- D. License & Contract and Package Repository

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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

QUESTION 128

To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

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



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 129

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

- A. All-in-one (stand-alone)
- B. CloudGuard
- C. Distributed
- D. Bridge Mode

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 130

Which of the following is NOT a valid backup command for a Security Management Server?

- A. save backup
- B. add backup
- C. add snapshot
- D. migrate export

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.networksecurityplus.net/2015/02/check-point-backup-and-restore-command-reference.html>

QUESTION 131

Which software blade does **NOT** accompany the Threat Prevention policy?

- A. Anti-virus
- B. IPS
- C. Threat Emulation
- D. Application Control and URL Filtering

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92707.htm



<https://vceplus.com/>

