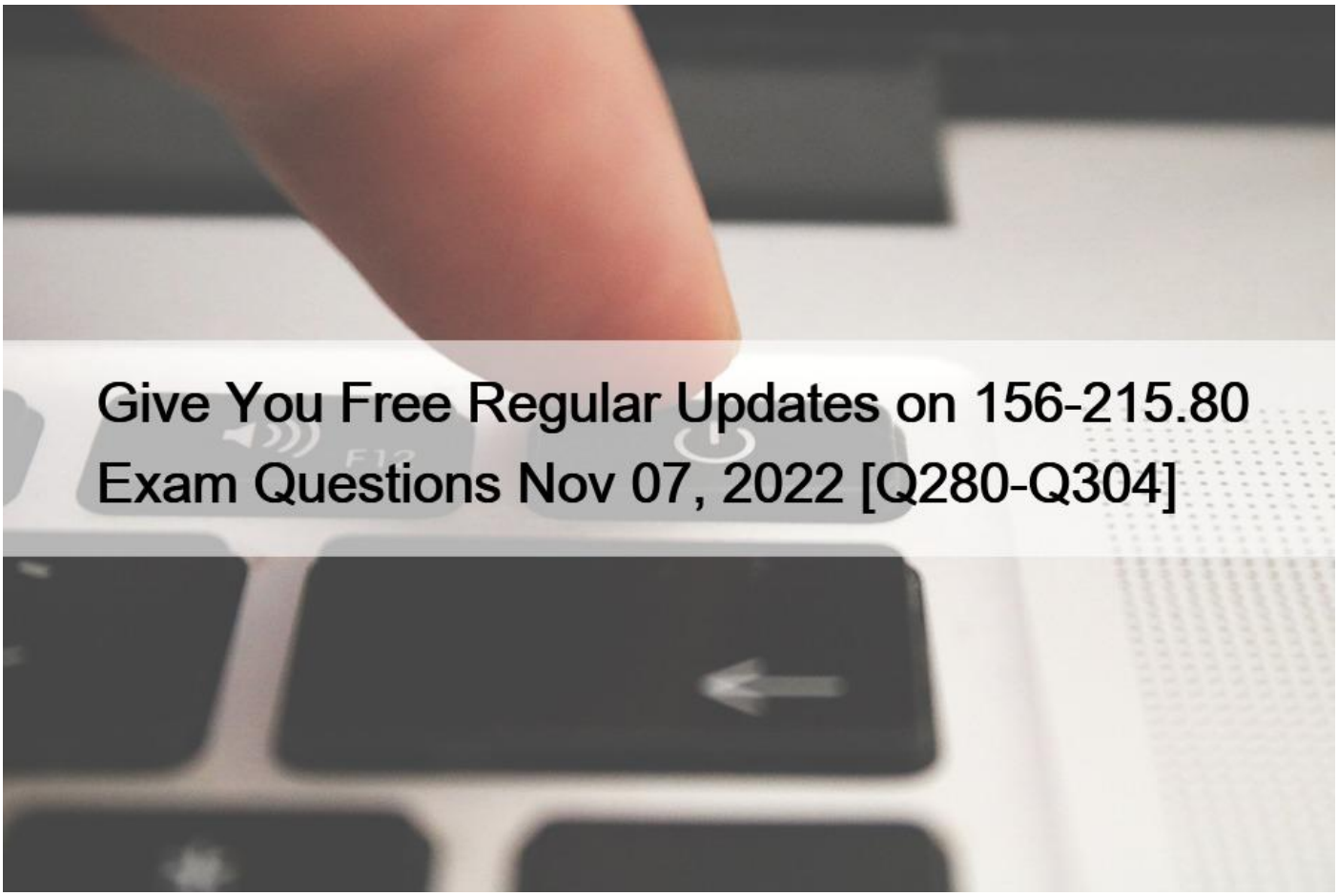
Give You Free Regular Updates on 156-215.80 Exam Questions Nov 07, 2022 [Q280-Q304



Give You Free Regular Updates on 156-215.80 Exam Questions Nov 07, 2022
Achieve the 156-215.80 Exam Best Results with Help from CheckPoint Certified Experts

Your Career Opportunities

The Check Point Certified Security Administrator is an amazing accomplishment that recognizes your ability to manage the Check Point products and services. On top of that, it will also qualify you for excellent job titles in the modern employment industry. It is even more satisfying to recall that all it takes to obtain such incredible opportunities is to pass one exam, known as the Check Point 156- According to the PayScale website, a typical CCSA certified individual earns an average salary of $85,216 annually. Here are the top job titles you can easily qualify for after acing this exam: - Systems Engineer;- Security Engineer;- Systems Administrator;- Security Analyst;- Network Engineer.

The Check Point 156-215.80 exam is a requirement for attaining the Check Point Certified Security Administrator certification (CCSA).

Check Point Certified Security Administrator (CCSA R80) 156-215.80 Exam

Check Point Certified Security Administrator (CCSA R80) 156-215.80 Exam is related to Check Point Certified Security Administrator Certification.156-215.80 Exam validates the ability to install R80 Management, security in a distributed environment configure objects rules, settings to define a security policy, work with multiple concurrent administrators and define permission

profiles. This exam also deals with the ability to configure a virtual private network, work with checkpoint clustering and perform periodic administrator tasks as specified in administrator job descriptions. Security Administrator and Check Point Professionals usually hold or pursue this certification and candidate can expect the same job roles after completion of this certification.

QUESTION 280

Phase 1 of the two-phase negotiation process conducted by IKE operates in _____ mode.
* Main
* Authentication
* Quick
* High Alert
Explanation

Phase I modes

Between Security Gateways, there are two modes for IKE phase I.

These modes only apply to IKEv1:

QUESTION 281

After the initial installation the First Time Configuration Wizard should be run.
* First Time Configuration Wizard can be run from the Unified SmartConsole.
* First Time Configuration Wizard can be run from the command line or from the WebUI.
* First time Configuration Wizard can only be run from the WebUI.
* Connection to the internet is required before running the First Time Configuration wizard.
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 282

Assuming you have a Distributed Deployment, what will be the effect of running the following command on the Security Management Server?

* Remove the installed Security Policy.

* Remove the local ACL lists.
* No effect.
* Reset SIC on all gateways.

Explanation

This command uninstall actual security policy (already installed)

QUESTION 283

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?
* To satellites through center only
* To center only
* To center and to other satellites through center
* To center, or through the center to other satellites, to internet and other VPN targets

Explanation

On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:

* To center and to other Satellites through center; this allows connectivity between Gateways; for example, if the spoke Gateways are DAIP Gateways, and the hub is a Gateway with a static IP address

* To center, or through the center to other satellites, to Internet and other VPN targets; this allows connectivity between the Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

References:

QUESTION 284

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

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

QUESTION 285

Which of the following is NOT a back up method?
* Save backup
* System backup
* snapshot
* Migrate

Explanation

The built-in Gaia backup procedures:

Check Point provides three different procedures for backing up (and restoring) the operating system and networking parameters on your appliances.

QUESTION 286

Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.
* SmartMonitor
* SmartView Web Application
* SmartReporter
* SmartTracker

Event Analysis with SmartEventThe 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. Withthe free-text search and suggestions, you can quickly run data analysis and identify critical security events.

QUESTION 287

What is the purpose of the Clean-up Rule?
* To log all traffic that is not explicitly allowed or denied in the Rule Base.
* To clean up policies found inconsistent with the compliance blade reports.
* To remove all rules that could have a conflict with other rules in the database.
* To eliminate duplicate log entries in the Security Gateway.

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.

QUESTION 288

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.

What is the possible explanation for this?
* 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.
* Another administrator is logged into the Management and currently editing the DNS Rule.
* DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.
* This is normal behavior in R80 when there are duplicate rules in the Rule Base.
Explanation/Reference:

QUESTION 289

R80 Security Management Server can be installed on which of the following operating systems?
* Gaia only
* Gaia, SPLAT, Windows Server only
* Gaia, SPLAT, Windows Server and IPSO only
* Gaia and SPLAT only
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

QUESTION 290

To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members?
* fw ctl set int fwha vmac global param enabled
* fw ctl get int fwha vmac global param enabled; result of command should return value 1
* cphaprob -a if
* fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1
Explanation/Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

QUESTION 291

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:
* assign privileges to users.
* edit the home directory of the user.
* add users to your Gaia system.
* assign user rights to their home directory in the Security Management Server
Explanation

Users

Use the WebUI and CLI to manage user accounts. You can:

QUESTION 292

In order to modify Security Policies, the administrator can use which of the following tools?
* Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
* SmartConsole and WebUI on the Security Management Server.
* mgmt_cli or WebUI on Security Gateway and SmartConsole on the Security Management Server.
* SmartConsole or mgmt_cli on any computer where SmartConsole is installed.

QUESTION 293

What does the “unknown” SIC status shown on SmartConsole mean?
* The SMS can contact the Security Gateway but cannot establish Secure Internal

Communication.
* SIC activation key requires a reset.
* The SIC activation key is not known by any administrator.
* There is no connection between the Security Gateway and SMS.

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.

QUESTION 294

Which of the following is NOT a VPN routing option available in a star community?
* To satellites through center only
* To center, or through the center to other satellites, to Internet and other VPN targets
* To center and to other satellites through center
* To center only

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:

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

QUESTION 295

Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.
* Block Port Overflow
* Local Interface Spoofing
* Suspicious Activity Monitoring
* Adaptive Threat Prevention

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 References:

QUESTION 296

What are the three tabs available in SmartView Tracker?
* Network & Endpoint, Management, and Active
* Network, Endpoint, and Active
* Predefined, All Records, Custom Queries
* Endpoint, Active, and Custom Queries

QUESTION 297

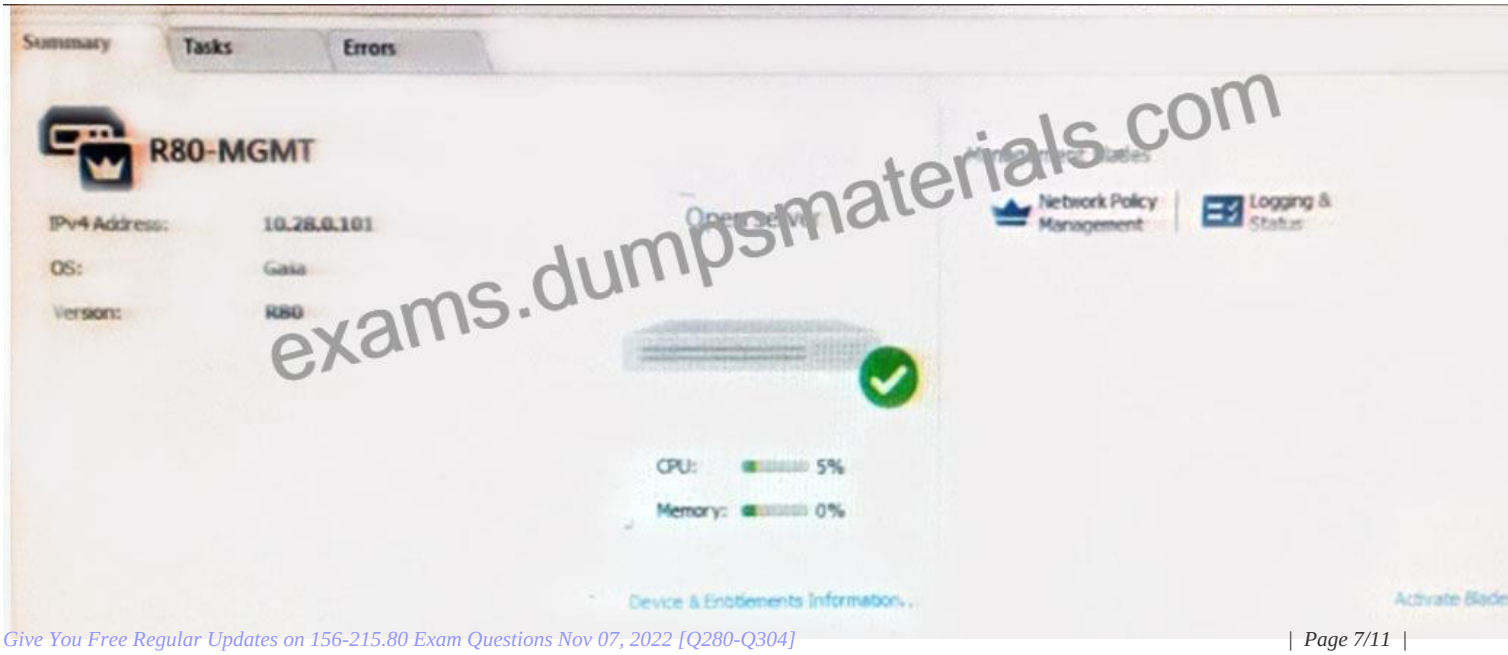
You have enabled “Extended Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?
* Logging has disk space issues. Change logging storage options on the logging server or Security Management Server properties and install database.
* Content Awareness is not enabled.
* Identity Awareness is not enabled.
* Log Trimming is enabled.

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 298

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.

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).

QUESTION 299

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

_____ .

* User Directory
* Captive Portal and Transparent Kerberos Authentication
* Captive Portal
* UserCheck

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 300

Look at the following screenshot and select the BEST answer.

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

QUESTION 301

Which of the following is NOT a back up method?
* Save backup
* System backup

snapshot
*
* Migrate
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 302

To build an effective Security Policy, use a _____ and _____ rule.
* Cleanup; stealth
* Stealth; implicit
* Cleanup; default
* Implicit; explicit
Explanation/Reference:

QUESTION 303

Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.
* 675, 389
* 389, 636
* 636, 290
* 290, 675
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 304

In which scenario is it a valid option to transfer a license from one hardware device to another?
* From a 4400 Appliance to an HP Open Server
* From an IBM Open Server to an HP Open Server
* From a 4400 Appliance to a 2200 Appliance
* From an IBM Open Server to a 2200 Appliance

Detailed New 156-215.80 Exam Questions for Concept Clearance:
https://www.dumpsmaterials.com/156-215.80-real-torrent.html]