156-215.75^{Q&As}

156-215.75$^{Q\&As}$

Check Point Certified Security Administrator

Pass CheckPoint 156-215.75 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/156-215-75.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

QUESTION 1

Which column in the Rule Base is used to define authentication parameters?

A. Source

B. Action

C. Track

D. Service

Correct Answer: B

QUESTION 2

SmartView Tracker logs the following Security Administrator activities, EXCEPT:

A. Administrator login and logout

B. Object creation, deletion, and editing

C. Tracking SLA compliance

D. Rule Base changes

Correct Answer: C

QUESTION 3

What is the primary benefit of using upgrade_export over either backup of snapshot?

A. The backup and snapshot commands can take long time to run whereas upgrade_export will take a much shorter amount of time.

B. upgrade_export will back up routing tables, hosts files, and manual ARP configurations, where backup and snapshot will not.

C. upgrade_export is operating system independent and can be used when backup or snapshot is not available.

D. upgrade_export has an option to backup the system and SmartView tracker logs while back and snapshot will not.

Correct Answer: C

QUESTION 4

Central license management allows a Security Administrator to perform which of the following functions?

1) Check for expired licenses. 2) Sort licenses and view license properties 3) Attach both R75 Central and Local

licenses to a remote module 4) Delete both R75 Local licenses and Central licenses from a remote module 5) Add or remove a license to or from the license repository 6) Attach and/or delete only R75 Central licenses to a remote module (not local licenses)

A. 2, 5, and 6

B. 2, 3, 4, and 5

C. 1, 2, 5, and 6

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

Correct Answer: D

QUESTION 5

Select the correct statement about Secure Internal Communications (SIC) Certificates. SIC Certificates:

A. Are used for securing internal network communications between the SmartDashboard and the Security Management Server.

B. For R75 Security Gateways are created during the Security Management Server installation.

C. Decrease network security by securing administrative communication among the Security Management Servers and the Security Gateway.

D. Uniquely identify Check Point enabled machines; they have the same function as VPN Certificates.

Correct Answer: D

QUESTION 6

Which feature or command provides the easiest path for Security Administrators to revert to earlier versions of the same Security Policy and objects configuration?

A. Policy Package management

B. dbexport/dbimport

C. Database Revision Control

D. upgrade_export/upgrade_import

Correct Answer: C

QUESTION 7

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

A. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.

B. Anti-spoofing not configured on the interfaces on the Gateway object.

C. A Gateway object created using the Check Point > Security Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

D. Secure Internal Communications (SIC) not configured for the object.

Correct Answer: A

QUESTION 8

When you hide a rule in a Rule Base, how can you then disable the rule?

A. Use the search utility in SmartDashboard to view all hidden rules Select the relevant rule and click Disable Rule(s).

B. Right-click on the hidden rule place-holder bar and select Disable Rule(s).

C. Right-click on the hidden rule place-holder bar and uncheck Hide, then right-click and select Disable Rule(s); re-hide the rule.

D. Hidden rules are already effectively disabled from Security Gateway enforcement.

Correct Answer: C

QUESTION 9

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

A. Install the View Implicit Rules package using SmartUpdate

B. Define two log serves on the R75 Gateway object Enable Log Implied Rules on the first log server. Enable Log Rule Base on the second log server. Use SmartReporter to merge the two log server records into the same database for HIPPA log audits.

C. In Global Properties > Reporting Tools check the box Enable tracking all rules (including rules marked as None in the Track column). Send these logs to a secondary log server for a complete logging history. Use your normal log server for standard logging for troubleshooting.

D. Check the Log Implied Rules Globally box on the R75 Gateway object.

Correct Answer: C

QUESTION 10

The Security Gateway is installed on SecurePlatform R75. The default port for the Web User Interface is _____.

A. TCP 18211

B. TCP 257

C. TCP 4433

D. TCP 443

Correct Answer: D

QUESTION 11

Of the three mechanisms Check Point uses for controlling traffic, which enables firewalls to incorporate layer 4 awareness in packet inspection?

A. IPS

B. Packet filtering

C. Stateful Inspection

D. Application Intelligence

Correct Answer: C

QUESTION 12

Reviews the following rules and note the Client Authentication Action properties screen, as shown below:

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

A. user is prompted from that FTP site only, and does not need to enter his username and password for Client Authentication.

B. User is prompted for Authentication by the Security Gateway again.

C. FTP data connection is dropped after the user is authenticated successfully.

D. FTP connection is dropped by rules 2.

Correct Answer: A

QUESTION 13

Where can an administrator configure the notification action in the event of a policy install time change?

A. SmartView Tracker / Audit Log

B. SmartView Monitor / Gateways / Thresholds Settings

C. SmartDashboard / Security Gateway Object / Advanced Properties Tab

D. SmartDashboard / Policy Package Manager

Correct Answer: B

QUESTION 14

Where is the best place to find information about connections between two machines?

A. On a Security Management Server, using SmartView Tracker

B. All options are valid.

C. On a Security Gateway using the command fw log.

D. On a Security Gateway Console interface; it gives you detailed access to log files and state table information

Correct Answer: A

QUESTION 15

When using LDAP as an authentication method for Identity Awareness, the query:

A. Prompts the user to enter credentials.

B. Requires administrators to specifically allow LDAP traffic to and from the LDAP Server and the Security Gateway.

C. Requires client and server side software.

D. Is transparent, requiring no client or server side software.

Correct Answer: D

Latest 156-215.75 Dumps   156-215.75 Practice Test   156-215.75 Study Guide