156-215.81.20^{Q&As}

156-215.81.20$^{Q\&As}$

Check Point Certified Security Administrator - R81.20 (CCSA)

Pass CheckPoint 156-215.81.20 Exam with 100% Guarantee

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

https://www.certbus.com/156-215-81-20.html

100% Passing Guarantee
100% Money Back Assurance

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Which tool allows you to monitor the top bandwidth on smart console?

A. Smart Event

B. Gateways and Servers Tab

C. SmartView Monitor

D. Logs and Monitoring

Correct Answer: C

QUESTION 2

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

A. Upper; Application

B. Lower; Application

C. First two; Internet

D. First two; Transport

Correct Answer: B

QUESTION 3

What is the user ID of a user that have all the privileges of a root user?

A. User ID 99

B. User ID 1

C. User ID 2

D. User ID 0

Correct Answer: D

QUESTION 4

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

A. SND is a feature to accelerate multiple SSL VPN connections

B. SND is an alternative to IPSec Main Mode, using only 3 packets

C. SND is used to distribute packets among Firewall instances

D. SND is a feature of fw monitor to capture accelerated packets

Correct Answer: C

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

---

QUESTION 5

Which of the following is used to enforce changes made to a Rule Base?

A. Publish database

B. Save changes

C. Install policy

D. Activate policy

Correct Answer: A

QUESTION 6

Where can I find the file for a Gaia backup named backup_fw on a Check Point Appliance?

A. /var/log/CPbackup/backups/backup_fw.tgz

B. /var/CPbackup/backups/backup_fw.tgz

C. /var/log/backups/backup_fw.tgz

D. $CPDIR/backups/backup_fw.tgz

Correct Answer: A

QUESTION 7

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

A. Firewall

B. Identity Awareness

C. Application Control

D. URL Filtering

Correct Answer: B

Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized

management and monitoring allows for policies to be managed from a single, unified console.

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

QUESTION 8

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

A. UserCheck

B. Active Directory Query

C. Account Unit Query

D. User Directory Query

Correct Answer: B

:

AD Query extracts user and computer identity information from the Active Directory Security Event Logs. The system generates a Security Event log entry when a user or computer accesses a network resource. For example, this occurs when

a user logs in, unlocks a screen, or accesses a network drive.

Reference : https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

---

QUESTION 9

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

A. Detects and blocks malware by correlating multiple detection engines before users are affected.

B. Configure rules to limit the available network bandwidth for specified users or groups.

C. Use UserCheck to help users understand that certain websites are against the company\\'s security policy.

D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Correct Answer: A

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

---

QUESTION 10

Which of these components does NOT require a Security Gateway R77 license?

A. Security Management Server

B. Check Point Gateway

C. SmartConsole

D. SmartUpdate upgrading/patching

Correct Answer: C

QUESTION 11

Which is a main component of the Check Point security management architecture?

A. Proxy Server

B. Endpoint VPN client

C. Identity Collector

D. SmartConsole

Correct Answer: D

QUESTION 12

Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.

B. One machine

C. Two machines D. Three machines

Correct Answer: C

One for Security Management Server and the other one for the Security Gateway.

QUESTION 13

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

QUESTION 14

When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

A. If the Action is Accept, the gateway allows the packet to pass through the gateway.

B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.

C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.

D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Correct Answer: C

QUESTION 15

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

A. Logout of the session

B. File > Save

C. Install database

D. Publish the session

Correct Answer: D

Installing and Publishing

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

You must do this: After you did this:

Publish Opened a session in SmartConsole and made changes.

The Publish operation sends all SmartConsole modifications to other

administrators, and makes the changes you made in a private session

public.

Install the database Modified network objects, such as servers, users, services, or IPS

profiles, but not the Rule Base.

Updates are installed on management servers and log servers.

Install a policy Changed the Rule Base.

The Security Management Server installs the updated policy and the

entire database on Security Gateways (even if you did not modify any

network objects).

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

Latest 156-215.81.20 Dumps   156-215.81.20 VCE Dumps   156-215.81.20 Practice Test