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.certbus.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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

The third shift administrator was updating security management server access setting in global properties. He managed to lock the entire Administrator out of their accounts. How should you unlock these accounts?

A. Logging to smart dash board as special cpconfig_admin account. Right click on each administrator object and select Unlock.

B. Type fwm lock_admin ua from the command line of the security management server

C. Reinstall the security management Server and restore using upgrade _imort

D. Delete the file admin .lock in the sfwdir/ tmp/directory of the security managem,ent server.

Correct Answer: B

QUESTION 2

You create implicit and explicit rules for the following network. The group object internal- networks includes networks 10.10.10.0 and 10.10.20.0. Assume Accept ICMP requests is enabled as Before last in Global Properties.

Based on these rules, what happens if you Ping from host 10.10.10.5 to a host on the Internet by IP address? ICMP will be:

A. dropped by rule 0.

B. dropped by rule 2, the Cleanup Rule.

C. accepted by rule 1.

D. dropped by the last Implicit rule.

Correct Answer: C

QUESTION 3

Which command allows verification of the Security Policy name and install date on a Security Gateway?

A. fw show policy

B. fw ctl pstat -policy

C. fw stat -l

D. fwver-p

Correct Answer: C

QUESTION 4

The London Security Gateway Administrator has just installed the Security Gateway and Management Server. He has not changed any default settings. As he tries to configure the Gateway, he is unable to connect. Which troubleshooting suggestion will NOT help him?

A. Check if some intermediate network device has a wrong routing table entry, VLAN assignment, duplex-mismatch, or trunk issue.

B. Verify that the Rule Base explicitly allows management connections.

C. Test the IP address assignment and routing settings of the Security Management Server, Gateway, and console client.

D. Verify the SIC initialization.

Correct Answer: B

QUESTION 5

What is the officially accepted diagnostic tool for IP appliance support?

A. Ipsinfo

B. Uag-diag

C. CST

D. cpinfo

Correct Answer: C

QUESTION 6

Once an Access Role is configured, in which Rule Bases can it be implemented?

A. DLP

B. Mobile Access

C. IPS

D. Application Control

Correct Answer: D

QUESTION 7

Which of the following statements about file-type recognition in Content Inspection is TRUE?

A. Antivirus status is monitored using SmartView Tracker.

B. A scan failure will only occur if the antivirus engine fails to initialize.

C. All file types are considered "at risk", and are not configurable by the Administrator or the Security Policy.

D. The antivirus engine acts as a proxy, caching the scanned file before delivering it to the client.

Correct Answer: D

QUESTION 8

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 9

In which directory do you install the R75 pre-upgrade verifier on a SecurePlatform Security Management Server?

A. It does not matter since the dynamic information entered by the Administrator will cause it to retrieve the proper configurations.

B. In $PWDIR/ conf.

C. It does not matter as long as the Administrator uses chmod to permit the file to execute.

D. in $PWDIR/ bin

Correct Answer: A

QUESTION 10

Which rule is responsible for installation feature?

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1	NetBIOS Rule	* Any	* Any	Any Traffic	NBT	drop	— None	* Policy Targets
2	Mgmt Rule	websignapore	fwsingapore	Any Traffic	TCP ssh TCP https	accept	Log	* Policy Targets
3	Stealth Rule	* Any	fwsingapore	Any Traffic	* Any	drop	Log	* Policy Targets
4	Client Auth Rule	websydney	websignapore	Any Traffic	TCP http	Client Auth	Log	* Policy Targets
5	Partner City Rule	net_singapore net_rome	net_singapore net_rome	Rome_Singapore	TCP http	accept	Log	* Policy Targets
6	Network Traffic Rule	net_singapore net_sydney	* Any	Any Traffic	dns TCP http	accept	Log	* Policy Targets
7	FTP Rule	* Any	websignapore	Any Traffic	TCP ftp	accept	Log	fwsydney
8	FTP Rule	* Any	websignapore	Any Traffic	TCP ftp	accept	Account	fwsingapore
9	Cleanup Rule	* Any	* Any	Any Traffic	* Any	drop	Log	* Policy Targets

A. Rule 4

B. Rule 8

C. Rule 7

D. Rule 5

Correct Answer: C

QUESTION 11

When a user selects to allow Hot-spot, SecureClient modifies the Desktop Security Policy and/or Hub Mode routing to enable Hot-spot registration. Which of the following is NOT true concerning this modification?

A. IP addresses accessed during registration are recorded.

B. Ports accessed during registration are recorded.

C. The number of IP addresses accessed is unrestricted.

D. The modification is restricted by time.

Correct Answer: C

QUESTION 12

You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? i.e. the command cprestart is not sufficient.

1.

Adding a hot-swappable NIC to the Operating System for the first time.

2.

Uninstalling the R75 Power/UTM package.

3.

Installing the R75 Power/UTM package.

4.

Re-establishing SIC to the Security Management Server.

5.

Doubling the maximum number of connections accepted by the Security Gateway.

A. 3 only

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

C. 2, 3 only

D. 3, 4, and 5 only

Correct Answer: C

QUESTION 13

To monitor all traffic between a network and the Internet on a SecurePlatform Gateway, what is the BEST utility to use?

A. snoop

B. cpinfo

C. infoview

D. tcpdump

Correct Answer: D

QUESTION 14

You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you

investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

A. Add a "temporary" rule using SmartDashboard and select hide rule.

B. Create a Suspicious Activity Rule in SmartView Monitor

C. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0. fws configuration file.

D. Select block intruder from the tools menu in SmartView Tracker.

Correct Answer: B

QUESTION 15

You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how often the particular rules match. Where can you see it? Give the BEST answer.

A. In SmartReporter, in the section Firewall Blade - Activity / Network Activity with information concerning Top Matched Logged Rules.

B. It is not possible to see it directly. You can open SmartDashboard and select UserDefined in the Track column. Afterwards, you need to create your own program with an external counter.

C. In the SmartView Tracker, if you activate the column Matching Rate.

D. SmartReporter provides this information in the section Firewall Blade - Security / Rule Base Analysis with information concerning Top Matched Logged Rules.

Correct Answer: D

[Latest 156-215.75 Dumps](#)   [156-215.75 VCE Dumps](#)   [156-215.75 Practice Test](#)