156-215.80 Q&As

Check Point Certified Security Administrator

Pass CheckPoint 156-215.80 Exam with 100% Guarantee

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

https://www.pass2lead.com/156-215-80.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

What is the command to see cluster status in cli expert mode?

A. fw ctl stat

B. clusterXL stat

C. clusterXL status

D. cphaprob stat

Correct Answer: A

QUESTION 2

What is the default shell for the command line interface?

A. Expert

B. Clish

C. Admin

D. Normal

Correct Answer: B

The default shell of the CLI is called clish Reference:
https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm

QUESTION 3

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap

B. Mail, Block Source, Block Destination, Block Services, SNMP Trap

C. Mail, Block Source, Block Destination, External Script, SNMP Trap

D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Correct Answer: A

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEvent_AdminGuide/17401.htm

QUESTION 4

SmartEvent does NOT use which of the following procedures to identity events:

A. Matching a log against each event definition

B. Create an event candidate

C. Matching a log against local exclusions

D. Matching a log against global exclusions

Correct Answer: C

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEvent_AdminGuide/17401.htm

QUESTION 5

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

QUESTION 6

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

A. User Directory

B. Captive Portal and Transparent Kerberos Authentication

C. Captive Portal

D. UserCheck

Correct Answer: B

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 7

What component of R80 Management is used for indexing?

A. DBSync

B. API Server

C. fwm

D. SOLR

Correct Answer: D

Reference: https://www.checkpoint.com/downloads/product-related/r80.10-mgmt-architecture-overview.pdf

QUESTION 8

What is the default method for destination NAT?

A. Destination side

B. Source side

C. Server side

D. Client side

Correct Answer: D

Client Side NAT - destination is NAT`d by the inbound kernel

QUESTION 9

Choose what BEST describes the Policy Layer Traffic Inspection.

A. If a packet does not match any of the inline layers, the matching continues to the next Layer.

B. If a packet matches an inline layer, it will continue matching the next layer.

C. If a packet does not match any of the inline layers, the packet will be matched against the Implicit Clean-up Rule.

D. If a packet does not match a Network Policy Layer, the matching continues to its inline layer.

Correct Answer: B

Reference: https://community.checkpoint.com/thread/1092

QUESTION 10

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

QUESTION 11

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

QUESTION 12

Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group,

and/or machine?

A. Application Control

B. Data Awareness

C. Identity Awareness

D. Threat Emulation

Correct Answer: A

QUESTION 13

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

QUESTION 14

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

QUESTION 15

Choose what BEST describes the reason why querying logs now is very fast.

A. New Smart-1 appliances double the physical memory install

B. Indexing Engine indexes logs for faster search results

C. SmartConsole now queries results directly from the Security Gateway

D. The amount of logs been store is less than the usual in older versions

Correct Answer: B