156-215.77^{Q&As}

Check Point Certified Security Administrator

Pass CheckPoint 156-215.77 Exam with 100% Guarantee

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

https://www.leads4pass.com/156-215-77.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 SmartView Tracker selection would most effectively show who installed a Security Policy blocking all traffic from the corporate network?

A. Management tab

B. Custom filter

C. Network and Endpoint tab

D. Active tab

Correct Answer: A

QUESTION 2

Where is the easiest and BEST place to find information about connections between two machines?

A. All options are valid.

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

C. On a Security Management Server, using SmartView Tracker.

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

Correct Answer: C

QUESTION 3

Which statement below describes the most correct strategy for implementing a Rule Base?

A. Limit grouping to rules regarding specific access.

B. Place the most frequently used rules at the top of the Policy and the ones that are not frequently used further down.

C. Place a network-traffic rule above the administrator access rule.

D. Add the Stealth Rule before the last rule.

Correct Answer: B

QUESTION 4

What happens if the identity of a user is known?

A. If the user credentials do not match an Access Role, the traffic is automatically dropped.

B. If the user credentials do not match an Access Role, the system displays a sandbox.

C. If the user credentials do not match an Access Role, the gateway moves onto the next rule.

D. If the user credentials do not match an Access Role, the system displays the Captive Portal.

Correct Answer: C

QUESTION 5

A _____ rule is used to prevent all traffic going to the R77 Security Gateway.

A. IPS

B. Cleanup

C. Reject

D. Stealth

Correct Answer: D

QUESTION 6

How do you recover communications between your Security Management Server and Security Gateway if you lock yourself out through a rule or policy mis-configuration?

A. fw unload policy

B. fw unloadlocal

C. fw delete all.all@localhost

D. fwm unloadlocal

Correct Answer: B

QUESTION 7

Exhibit:

Latest 156-215.77 Dumps | 156-215.77 VCE Dumps | 156-215.77 Practice Test

Chris has lost SIC communication with his Security Gateway and he needs to re-establish SIC. What would be the correct order of steps needed to perform this task?

A. 5, 1, 2, 4

B. 5, 1, 4, 2

C. 3, 1, 4, 2

D. 2, 3, 1, 4

Correct Answer: A

QUESTION 8

Static NAT connections, by default, translate on which firewall kernel inspection point?

A. Inbound

B. Outbound

C. Post-inbound

D. Eitherbound

Correct Answer: A

QUESTION 9

What is the syntax for uninstalling a package using newpkg?

A. -u

B. -i

C. -S

D. newpkg CANNOT be used to uninstall a package

Correct Answer: D

QUESTION 10

Which of the following uses the same key to decrypt as it does to encrypt?

A. B. Dynamic encryption

B. C. Certificate-based encryption

C. D. Symmetric encryption

Correct Answer: A

QUESTION 11

How granular may an administrator filter an Access Role with identity awareness? Per:

A. Specific ICA Certificate

B. AD User

C. Radius Group

D. Windows Domain

Correct Answer: B

QUESTION 12

As you review this Security Policy, what changes could you make to accommodate Rule 4? Exhibit:

No.	Hits	Name	Source	Destination	VPN	Service	Action
⊟	Limit Access to Gateways (Rule 1)						
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
⊟	VPN Access Rules (Rules 2-5)						
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS, ftp-port, http, https, smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS, http, https, imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth
5	0	Web Server	L2TP-vpn-user@Any, Customers@Any	Remote-1-web-server	Any Traffic	http	accept

A. Remove the service HTTP from the column Service in Rule 4.

B. Modify the column VPN in Rule 2 to limit access to specific traffic.

C. Nothing at all

D. Modify the columns Source or Destination in Rule 4.

Correct Answer: B

QUESTION 13

Which of the following R77 SmartView Tracker views will display a popup warning about performance implications on the Security Gateway?

A. All Records Query

B. Account Query

C. Active Tab

D. Audit Tab

Correct Answer: C

QUESTION 14

Suppose the Security Gateway hard drive fails and you are forced to rebuild it. You have a snapshot file stored to a TFTP server and backups of your Security Management Server. What is the correct procedure for rebuilding the Gateway quickly?

A. Reinstall the base operating system (i.e., GAiA). Configure the Gateway interface so that the Gateway can communicate with the TFTP server. Revert to the stored snapshot image, and install the Security Policy.

B. Run the command revert to restore the snapshot, establish SIC, and install the Policy.

C. Run the command revert to restore the snapshot. Reinstall any necessary Check Point products. Establish SIC and install the Policy.

D. Reinstall the base operating system (i.e., GAia). Configure the Gateway interface so that the Gateway can communicate with the TFTP server. Reinstall any necessary Check Point products and previously applied hotfixes. Revert to the stored snapshot image, and install the Policy.

Correct Answer: A

QUESTION 15

What command syntax would you use to turn on PDP logging in a distributed environment?

A. pdp track=1

B. pdp tracker on

C. pdp logging on

D. pdp log=1

Correct Answer: B

[Latest 156-215.77 Dumps](#)   [156-215.77 VCE Dumps](#)   [156-215.77 Practice Test](#)