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.pass2lead.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

QUESTION 1

Which SmartView Tracker mode allows you to read the SMTP e-mail body sent from the Chief Executive Officer (CEO) of a company?

A. This is not a SmartView Tracker feature.

B. Display Capture Action

C. Network and Endpoint Tab

D. Display Payload View

Correct Answer: A

QUESTION 2

You are a Security Administrator who has installed Security Gateway R77 on your network. You need to

allow a specific IP address range for a partner site to access your intranet Web server. To limit the

partner\\'s access for HTTP and FTP only, you did the following:

1) Created manual Static NAT rules for the Web server.

2) Cleared the following settings in the Global Properties > Network Address Translation screen:

-Allow bi-directional NAT

-

Translate destination on client side Do the above settings limit the partner\\'s access?

A.

Yes. This will ensure that traffic only matches the specific rule configured for this traffic, and that the Gateway translates the traffic after accepting the packet.

B.

No. The first setting is not applicable. The second setting will reduce performance.

C.

Yes. Both of these settings are only applicable to automatic NAT rules.

D.

No. The first setting is only applicable to automatic NAT rules. The second setting will force translation by the kernel on the interface nearest to the client.

Correct Answer: D

QUESTION 3

When attempting to connect with SecureClient Mobile you get the following error message: The certificate provided is invalid. Please provide the username and password. What is the probable cause of the error?

A. Your user configuration does not have an office mode IP address so the connection failed.

B. Your certificate is invalid.

C. There is no connection to the server, and the client disconnected.

D. Your user credentials are invalid.

Correct Answer: B

QUESTION 4

You review this Security Policy because Rule 4 is inhibited. Which Rule is responsible? 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. No rule inhibits Rule 4.

B. Rule 1

C. Rule 2

D. Rule 3

Correct Answer: C

QUESTION 5

One of your remote Security Gateways suddenly stops sending logs, and you cannot install the Security Policy on the

Gateway. All other remote Security Gateways are logging normally to the Security Management Server, and Policy installation is not affected. When you click the Test SIC status button in the problematic Gateway object, you receive an error message. What is the problem?

A. The remote Gateway\\'s IP address has changed, which invalidates the SIC Certificate.

B. The time on the Security Management Server\\'s clock has changed, which invalidates the remote Gateway\\'s Certificate.

C. The Internal Certificate Authority for the Security Management Server object has been removed from objects_5_0.c.

D. There is no connection between the Security Management Server and the remote Gateway. Rules or routing may block the connection.

Correct Answer: D

QUESTION 6

Which SmartConsole component can Administrators use to track changes to the Rule Base?

A. WebUI

B. SmartView Tracker

C. SmartView Monitor

D. SmartReporter

Correct Answer: B

QUESTION 7

Your Security Gateways are running near performance capacity and will get upgraded hardware next week. Which of the following would be MOST effective for quickly dropping all connections from a specific attacker\\'s IP at a peak time of day?

A. Intrusion Detection System (IDS) Policy install

B. Change the Rule Base and install the Policy to all Security Gateways

C. SAM - Block Intruder feature of SmartView Tracker

D. SAM - Suspicious Activity Rules feature of SmartView Monitor

Correct Answer: D

QUESTION 8

You are about to test some rule and object changes suggested in an R77 news group. Which backup solution should you use to ensure the easiest restoration of your Security Policy to its previous configuration after testing the changes?

A. Manual copies of the directory $FWDIR/conf

B. upgrade_export command

C. Database Revision Control

D. GAiA backup utilities

Correct Answer: C

QUESTION 9

Which of the following is a viable consideration when determining Rule Base order?

A. Grouping IPS rules with dynamic drop rules

B. Placing more restrictive rules before more permissive rules

C. Grouping authentication rules with QOS rules

D. Grouping reject and drop rules after the Cleanup Rule

Correct Answer: B

QUESTION 10

You have installed a R77 Security Gateway on GAiA. To manage the Gateway from the enterprise Security Management Server, you create a new Gateway object and Security Policy. When you install the new Policy from the Policy menu, the Gateway object does not appear in the Install Policy window as a target. What is the problem?

A. The object was created with Node > Gateway.

B. No Masters file is created for the new Gateway.

C. The Gateway object is not specified in the first policy rule column Install On.

D. The new Gateway\\'s temporary license has expired.

Correct Answer: A

QUESTION 11

SmartView Tracker R77 consists of three different modes. They are:

A. Log, Active, and Audit

B. Log, Active, and Management

C. Network and Endpoint, Active, and Management

D. Log, Track, and Management

Correct Answer: C

QUESTION 12

Where can you find the Check Point\\'s SNMP MIB file?

A. $CPDIR/lib/snmp/chkpt.mib

B. $FWDIR/conf/snmp.mib

C. It is obtained only by request from the TAC.

D. There is no specific MIB file for Check Point products.

Correct Answer: A

QUESTION 13

Sally has a Hot Fix Accumulator (HFA) she wants to install on her Security Gateway which operates with GAiA, but she cannot SCP the HFA to the system. She can SSH into the Security Gateway, but she has never been able to SCP files to it. What would be the most likely reason she cannot do so?

A. She needs to edit /etc/SSHd/SSHd_config and add the Standard Mode account.

B. She needs to run sysconfig and restart the SSH process.

C. She needs to edit /etc/scpusers and add the Standard Mode account.

D. She needs to run cpconfig to enable the ability to SCP files.

Correct Answer: C

QUESTION 14

Which of the following statements accurately describes the command snapshot?

A. snapshot creates a full OS-level backup, including network-interface data, Check Point product information, and configuration settings during an upgrade of a GAiA Security Gateway.

B. snapshot creates a Security Management Server full system-level backup on any OS.

C. snapshot stores only the system-configuration settings on the Gateway.

D. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server.

Correct Answer: A

QUESTION 15

You are working with multiple Security Gateways that enforce an extensive number of rules. To simplify security administration, which one of the following would you choose to do?

A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.

B. Run separate SmartConsole instances to login and configure each Security Gateway directly.

C. Create network objects that restrict all applicable rules to only certain networks.

D. Create a separate Security Policy package for each remote Security Gateway.

Correct Answer: D