



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:

<http://www.CertBus.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
-  **80000+** Satisfied Customers



Vendor: Check Point

Exam Code: 156-215.77

Exam Name: Check Point Certified Security Administrator

Q&As: Demo

QUESTION 1

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 2

Can you use Captive Portal with HTTPS?

- A. No, it only works with FTP
- B. No, it only works with FTP and HTTP
- C. Yes
- D. No, it only works with HTTP

Correct Answer: C

QUESTION 3

Which of the following is NOT defined by an Access Role object?

- A. Source Network
- B. Source Machine
- C. Source User
- D. Source Server

Correct Answer: D

QUESTION 4

In which Rule Base can you implement an Access Role?

- A. DLP
- B. Mobile Access
- C. IPS
- D. Firewall

Correct Answer: D

QUESTION 5

Access Role objects define users, machines, and network locations as:

- A. Credentialed objects
- B. Linked objects
- C. One object
- D. Separate objects

Correct Answer: C

QUESTION 6

Where do you verify that UserDirectory is enabled?

- A. Verify that Security Gateway > General Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked

- B. Verify that Global Properties > Authentication > Use UserDirectory (LDAP) for Security Gateways is checked
- C. Verify that Security Gateway > General Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked
- D. Verify that Global Properties > UserDirectory (LDAP) > Use UserDirectory (LDAP) for Security Gateways is checked

Correct Answer: D

QUESTION 7

Which of the following statements is TRUE about management plug-ins?

- A. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
- B. Installing a management plug-in is just like an upgrade process.
- C. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.
- D. The plug-in is a package installed on the Security Gateway.

Correct Answer: A

QUESTION 8

Which command displays the installed Security Gateway version?

- A. fw printver
- B. fw ver
- C. fw stat
- D. cpstat -gw

Correct Answer: B

QUESTION 9

Which command line interface utility allows the administrator to verify the Security Policy name and timestamp currently installed on a firewall module?

- A. cpstat fwd
- B. fw ver
- C. fw stat
- D. fw ctl pstat

Correct Answer: C

QUESTION 10

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 11

Which of the following statements accurately describes the command `upgrade_export`?

- A. `upgrade_export` stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.
- B. Used primarily when upgrading the Security Management Server, `upgrade_export` stores all object databases and the `/conf` directories for importing to a newer Security Gateway version.
- C. `upgrade_export` is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.
- D. This command is no longer supported in GAIa.

Correct Answer: B

QUESTION 12

What are you required to do before running the command `upgrade_export`?

- A. Run a `cpstop` on the Security Gateway.
- B. Run a `cpstop` on the Security Management Server.
- C. Close all GUI clients.
- D. Run `cpconfig` and set yourself up as a GUI client.

Correct Answer: C

QUESTION 13

A snapshot delivers a complete GAIa backup. The resulting file can be stored on servers or as a local file in `/var/CPsnapshot/snapshots`. How do you restore a local snapshot named `MySnapshot.tgz`?

- A. Reboot the system and call the start menu. Select the option Snapshot Management, provide the Expert password and select [L] for a restore from a local file. Then, provide the correct file name.
- B. As expert user, type the command `snapshot -r MySnapshot.tgz`.
- C. As expert user, type the command `revert --file MySnapshot.tgz`.
- D. As expert user, type the command `snapshot -R` to restore from a local file. Then, provide the correct file name.

Correct Answer: C

QUESTION 14

What is the primary benefit of using the command `upgrade_export` over either `backup` or `snapshot`?

- A. `upgrade_export` is operating system independent and can be used when `backup` or `snapshot` is not available.
- B. `upgrade_export` will back up routing tables, hosts files, and manual ARP configurations, where `backup` and `snapshot` will not.
- C. The commands `backup` and `snapshot` can take a long time to run whereas `upgrade_export` will take a much shorter amount of time.
- D. `upgrade_export` has an option to back up the system and SmartView Tracker logs while `backup` and `snapshot` will not.

Correct Answer: A

QUESTION 15

Which set of objects have an Authentication tab?

- A. Templates, Users
- B. Users, Networks
- C. Users, User Groups
- D. Networks, Hosts

Correct Answer: A

QUESTION 16

How are cached usernames and passwords cleared from the memory of a R77 Security Gateway?

- A. By using the Clear User Cache button in SmartDashboard.
- B. Usernames and passwords only clear from memory after they time out.
- C. By retrieving LDAP user information using the command fw fetchldap.
- D. By installing a Security Policy.

Correct Answer: D

QUESTION 17

Your users are defined in a Windows 2008 R2 Active Directory server. You must add LDAP users to a Client Authentication rule. Which kind of user group do you need in the Client Authentication rule in R77?

- A. External-user group
- B. LDAP group
- C. A group with a generic user
- D. All Users

Correct Answer: B

QUESTION 18

Assume you are a Security Administrator for ABCTech. You have allowed authenticated access to users from Mktng_net to Finance_net. But in the user's properties, connections are only permitted within Mktng_net. What is the BEST way to resolve this conflict?

- A. Select Ignore Database in the Action Properties window.
- B. Permit access to Finance_net.
- C. Select Intersect with user database in the Action Properties window.
- D. Select Intersect with user database or Ignore Database in the Action Properties window.

Correct Answer: D

QUESTION 19

For remote user authentication, which authentication scheme is NOT supported?

- A. Check Point Password
- B. RADIUS
- C. TACACS
- D. SecurID

Correct Answer: C

QUESTION 20

Review the rules.

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	TCP http TCP ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets

Assume domain UDP is enabled in the implied rules.

What happens when a user from the internal network tries to browse to the internet using HTTP? The user:

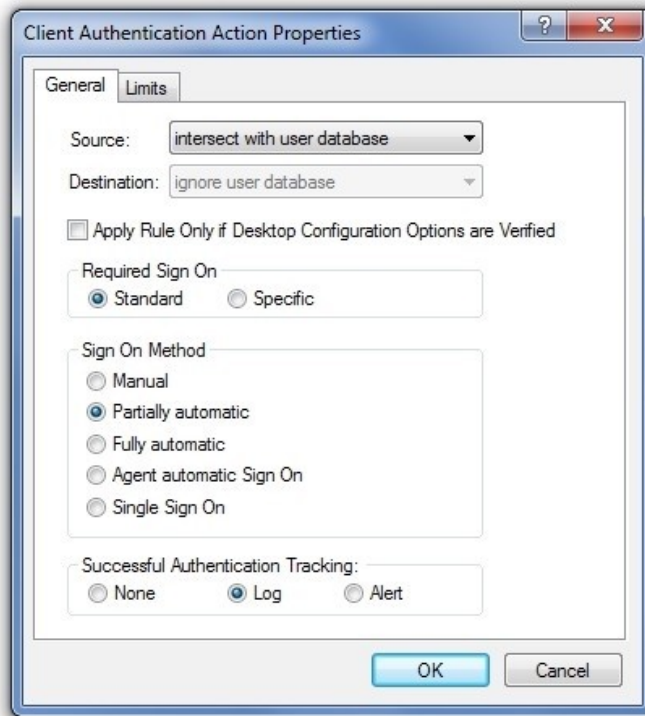
- A. can connect to the Internet successfully after being authenticated.
- B. is prompted three times before connecting to the Internet successfully.
- C. can go to the Internet after Telnetting to the client authentication daemon port 259.
- D. can go to the Internet, without being prompted for authentication.

Correct Answer: D

QUESTION 21

Study the Rule base and Client Authentication Action properties screen -

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	TCP http TCP ftp TCP telnet	Client Aut	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	drop	Log	Policy Targets



After being authenticated by the Security Gateway, when a user starts an HTTP connection to a Web site, the user tries to FTP to another site using the command line. What happens to the user?

- A. user is prompted for authentication by the Security Gateway again.
- B. FTP data connection is dropped after the user is authenticated successfully.
- C. user is prompted to authenticate from that FTP site only, and does not need to enter his username and password for Client Authentication.
- D. FTP connection is dropped by Rule 2.

Correct Answer: C

QUESTION 22

One of your remote Security Gateway's 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 23

What information is found in the SmartView Tracker Management log?

- A. SIC revoke certificate event
- B. Destination IP address
- C. Most accessed Rule Base rule
- D. Number of concurrent IKE negotiations

Correct Answer: A

QUESTION 24

What information is found in the SmartView Tracker Management log?

- A. Historical reports log
- B. Policy rule modification date/time stamp
- C. Destination IP address
- D. Most accessed Rule Base rule

Correct Answer: B

QUESTION 25

What information is found in the SmartView Tracker Management log?

- A. Creation of an administrator using cpconfig
- B. GAIa expert login event
- C. FTP username authentication failure
- D. Administrator SmartDashboard logout event

Correct Answer: D

QUESTION 26

How do you use SmartView Monitor to compile traffic statistics for your company's Internet Web activity during production hours?

- A. Select Tunnels view, and generate a report on the statistics.
- B. Configure a Suspicious Activity Rule which triggers an alert when HTTP traffic passes through the Gateway.
- C. Use Traffic settings and SmartView Monitor to generate a graph showing the total HTTP traffic for the day.
- D. View total packets passed through the Security Gateway.

Correct Answer: C

QUESTION 27

Which R77 SmartConsole tool would you use to verify the installed Security Policy name on a Security Gateway?

- A. SmartView Monitor
- B. SmartUpdate
- C. SmartView Status
- D. None, SmartConsole applications only communicate with the Security Management Server.

Correct Answer: A

QUESTION 28

Which R77 GUI would you use to see the number of packets accepted since the last policy install?

- A. SmartView Monitor
- B. SmartView Tracker
- C. SmartDashboard
- D. SmartView Status

Correct Answer: A

QUESTION 29

You are trying to save a custom log query in R77 SmartView Tracker, but getting the following error:

Could not save <query-name> (Error: Database is Read Only)

Which of the following is a likely explanation for this?

- A. Another administrator is currently connected to the Security Management Server with read/write permissions which impacts your ability to save custom log queries to the Security Management Server.
- B. You do not have OS write permissions on the local SmartView Tracker PC in order to save the custom query locally.
- C. You have read-only rights to the Security Management Server database.
- D. You do not have the explicit right to save a custom query in your administrator permission profile under SmartConsole customization.

Correct Answer: C

QUESTION 30

The R77 fw monitor utility is used to troubleshoot which of the following problems?

- A. Traffic issues
- B. Log Consolidation Engine
- C. User data base corruption
- D. Phase two key negotiation

Correct Answer: A

QUESTION 31

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 the SmartView Tracker, if you activate the column Matching Rate.
- B. In SmartReporter, in the section Firewall Blade - Activity > Network Activity with information concerning Top Matched Logged Rules.
- C. SmartReporter provides this information in the section Firewall Blade - Security > Rule Base Analysis

with information concerning Top Matched Logged Rules.

- D. 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.

Correct Answer: C

QUESTION 32

A company has disabled logging for some of the most commonly used Policy rules. This was to decrease load on the Security Management Server and to make tracking dropped connections easier. What action would you recommend to get reliable statistics about the network traffic using SmartReporter?

- A. SmartReporter analyzes all network traffic, logged or not.
- B. Network traffic cannot be analyzed when the Security Management Server has a high load.
- C. Turn the field Track of each rule to LOG.
- D. Configure Additional Logging on an additional log server.

Correct Answer: D

QUESTION 33

What is a Consolidation Policy?

- A. The collective name of the Security Policy, Address Translation, and IPS Policies.
- B. The specific Policy written in SmartDashboard to configure which log data is stored in the SmartReporter database.
- C. The collective name of the logs generated by SmartReporter.
- D. A global Policy used to share a common enforcement policy for multiple Security Gateways.

Correct Answer: B

QUESTION 34

Which feature in R77 permits blocking specific IP addresses for a specified time period?

- A. Suspicious Activity Monitoring
- B. HTTP Methods
- C. Local Interface Spoofing
- D. Block Port Overflow

Correct Answer: A

QUESTION 35

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 36

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 37

What port is used for communication to the User Center with SmartUpdate?

- A. CPMI 200
- B. TCP 8080
- C. HTTP 80
- D. HTTPS 443

Correct Answer: D

QUESTION 38

You are a Security Administrator preparing to deploy a new HFA (Hotfix Accumulator) to ten Security Gateways at five geographically separate locations. What is the BEST method to implement this HFA?

- A. Use a SSH connection to SCP the HFA to each Security Gateway. Once copied locally, initiate a remote installation command and monitor the installation progress with SmartView Monitor.
- B. Send a CD-ROM with the HFA to each location and have local personnel install it.
- C. Send a Certified Security Engineer to each site to perform the update.
- D. Use SmartUpdate to install the packages to each of the Security Gateways remotely.

Correct Answer: D

QUESTION 39

What action can be performed from SmartUpdate R77?

- A. upgrade_export
- B. fw stat -l
- C. cpinfo
- D. remote_uninstall_verifier

Correct Answer: C

QUESTION 40

Which tool CANNOT be launched from SmartUpdate R77?

- A. IP Appliance Voyager
- B. snapshot
- C. GAIa WebUI
- D. cpinfo

Correct Answer: B

QUESTION 41

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 42

Which of the following are available SmartConsole clients which can be installed from the R77 Windows CD? Read all answers and select the most complete and valid list.

- A. SmartView Tracker, SmartDashboard, CPINFO, SmartUpdate, SmartView Status
- B. SmartView Tracker, SmartDashboard, SmartLSM, SmartView Monitor
- C. SmartView Tracker, CPINFO, SmartUpdate
- D. Security Policy Editor, Log Viewer, Real Time Monitor GUI

Correct Answer: C

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Trying our product !

- ★ **100%** Guaranteed Success
- ★ **100%** Money Back Guarantee
- ★ **365 Days** Free Update
- ★ **Instant Download** After Purchase
- ★ **24x7** Customer Support
- ★ Average **99.9%** Success Rate
- ★ More than **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 One Year Free Update <p>Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 Money Back Guarantee <p>To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 Security & Privacy <p>We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

[Guarantee & Policy](#) | [Privacy & Policy](#) | [Terms & Conditions](#)

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © 2004-2017, All Rights Reserved.