EXAM 156-315.77

Check Point Certified Security Expert (CCSE) R77 Certification

Question: 1

Control connections between the Security Management Server and the Gateway are not encrypted by the VPN Community. How are these connections secured?

A. They are encrypted and authenticated using SIC.
B. They are not encrypted, but are authenticated by the Gateway
C. They are secured by PPTP
D. They are not secured.

Answer: D

Question: 2

If Bob wanted to create a Management High Availability configuration, what is the minimum number of Security Management servers required in order to achieve his goal?

A. Three
B. Two
C. Four
D. One

Answer: D

Question: 3

David wants to manage hundreds of gateways using a central management tool. What tool would David use to accomplish his goal?

A. SmartProvisioning
B. SmartBlade
C. SmartDashboard
D. SmartLSM

Answer: B

Question: 4

From the following output of cphaprob state, which ClusterXL mode is this?

```
Number          Unique IP Address       Assigned Load       State
1 (local)       192.168.1.1             30%                 active
2               192.168.1.2             70%                 active
```

A. New mode
B. Multicast mode
C. Legacy mode
D. Unicast mode

Answer: D

Question: 5

Which of the following is NOT a feature of ClusterXL?

A. Enhanced throughput in all ClusterXL modes (2 gateway cluster compared with 1 gateway)
B. Transparent failover in case of device failures
C. Zero downtime for mission-critical environments with State Synchronization
D. Transparent upgrades

Answer: C

Question: 6

In which case is a Sticky Decision Function relevant?

A. Load Sharing - Unicast
B. Load Balancing - Forward
C. High Availability
D. Load Sharing - Multicast

Answer: C

Question: 7

You configure a Check Point QoS Rule Base with two rules: an HTTP rule with a weight of 40, and the Default Rule with a weight of 10. If the only traffic passing through your QoS Module is HTTP traffic, what percent of bandwidth will be allocated to the HTTP traffic?

A. 80%
B. 40%
C. 100%
D. 50%

Answer: D

Question: 8

You have pushed a policy to your firewall and you are not able to access the firewall. What command will allow you to remove the current policy from the machine?

A. fw purge policy
B. fw fetch policy
C. fw purge active
D. fw unloadlocal

Answer: A

Question: 9

How do you verify the Check Point kernel running on a firewall?

A. fw ctl get kernel
B. fw ctl pstat
C. fw kernel
D. fw ver -k

Answer: B

Question: 10

The process _____ compiles $FWDIR/conf/*.W files into machine language.

A. fw gen
B. cpd
C. fwd
D. fwm

Answer: A

Question: 11

Which of the following is NOT part of the policy installation process?

A. Code compilation
B. Code generation
C. Initiation
D. Validation

Answer: D

Question: 12

When, during policy installation, does the atomic load task run?

A. It is the first task during policy installation.
B. It is the last task during policy installation.
C. Before CPD runs on the Gateway.
D. Immediately after fwm load runs on the SmartCenter.

Answer: B

Question: 13

What process is responsible for transferring the policy file from SmartCenter to the Gateway?

A. FWD
B. FWM
C. CPRID
D. CPD

Answer: D

Question: 14

What firewall kernel table stores information about port allocations for Hide NAT connections?

A. NAT_dst_any_list
B. host_ip_addrs
C. NAT_src_any_list
D. fwx_alloc

Answer: D

Question: 15

Where do you define NAT properties so that NAT is performed either client side or server side?

A. In SmartDashboard under Gateway setting
B. In SmartDashboard under Global Properties > NAT definition
C. In SmartDashboard in the NAT Rules
D. In file $DFWDIR/lib/table.def

Answer: B

Question: 16

The process _____ is responsible for all other security server processes run on the Gateway.

A. FWD
B. CPLMD
C. FWM
D. CPD

Answer: A

Question: 17

The process _____ is responsible for GUIClient communication with the SmartCenter.

A. FWD
B. FWM
C. CPD
D. CPLMD

Answer: B

Question: 18

The process _____ is responsible for Policy compilation.

A. FWM
B. Fwcmp
C. CPLMD
D. CPD

Answer: A

Question: 19

The process _____ is responsible for Management High Availability synchronization.

A. CPLMD
B. FWM
C. Fwsync
D. CPD

Answer: B

Question: 20

_____ is the called process that starts when opening SmartView Tracker application.

A. logtrackerd
B. fwlogd
C. CPLMD
D. FWM

Answer: C

Question: 21

Anytime a client initiates a connection to a server, the firewall kernel signals the FWD process using a trap. FWD spawns the _____ child service, which runs the security server.

A. FWD
B. FWSD
C. In.httpd
D. FWSSD

Answer: D

Question: 22

Security server configuration settings are stored in _____ .

A. $FWDIR/conf/AMT.conf
B. $FWDIR/conf/fwrl.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/conf/fwopsec.conf

Answer: C

Question: 23

User definitions are stored in _____ .

A. $FWDIR/conf/fwmuser
B. $FWDIR/conf/users.NDB
C. $FWDIR/conf/fwauth.NDB
D. $FWDIR/conf/fwusers.conf

Answer: C

Question: 24

Jon is explaining how the inspection module works to a colleague. If a new connection passes through the inspection module and the packet matches the rule, what is the next step in the process?

A. Verify if the packet should be moved through the TCP/IP stack.
B. Verify if any logging or alerts are defined.
C. Verify if the packet should be rejected.
D. Verify if another rule exists.

Answer: B

Question: 25

Which of the following statements accurately describes the upgrade_export command?

A. Used primarily when upgrading the Security Management Server, upgrade_export stores all object databases and the conf directories for importing to a newer version of the Security Gateway.
B. Used when upgrading the Security Gateway, upgrade_export includes modified files, such as in the directories /lib and /conf.
C. upgrade_export is used when upgrading the Security Gateway, and allows certain files to be included or excluded before exporting.
D. upgrade_export stores network-configuration data, objects, global properties, and the database revisions prior to upgrading the Security Management Server.

Answer: A

Question: 26

What are you required to do before running upgrade_export?

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

Answer: D

Question: 27

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

Answer: B

Question: 28

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

A. The commands backup and snapshot can take a 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 has an option to backup the system and SmartView Tracker logs while backup and snapshot will not.
D. upgrade_export is operating system independent and can be used when backup or snapshot is not available.

Answer: D

Question: 29

Your R7x-series Enterprise Security Management Server is running abnormally on Windows Server 2003 R2. You decide to try reinstalling the Security Management Server, but you want to try keeping the critical Security Management Server configuration settings intact (i.e., all Security Policies, databases, SIC, licensing etc.) What is the BEST method to reinstall the Server and keep its critical configuration?
A)

1. Run `cpstop` on one member, and configure the new interface via `sysconfig`.
2. Run `cpstart` on the cluster member. Repeat the same steps on another member.
3. Update the new topology in the cluster object from SmartDashboard.
4. Install the Security Policy.

B)

1. Use the `ifconfig` command to configure and enable the new interface on both members.
2. Run `cprestart` on both members.
3. Update the topology in the cluster object for the cluster and both members.
4. Install the Security Policy.

C)

1. Use `sysconfig` to configure the new interfaces on both members.
2. Update the topology in the cluster object.
3. Install the Security Policy.

D)

1. Disable "Cluster membership" from one gateway via `cpconfig`.
2. Configure the new interface via `sysconfig` from the "non-member" Gateway.
3. Re-enable "Cluster membership" on the Gateway.
4. Perform the same steps on the other Gateway.
5. Update the topology in the cluster object.
6. Install the Security Policy.

A. Exhibit A
B. Exhibit B
C. Exhibit C
D. Exhibit D

Answer: B

Question: 30

Your primary Security Management Server runs on SecurePlatform. What is the easiest way to back up your Security Gateway R75 configuration, including routing and network configuration files?

A. Using the native SecurePlatform back up utility from command line or in the Web-based user interface.
B. Using the command upgrade_export.
C. Run the command pre_upgrade_verifier and save the file *.tgz to the directory c:/temp.
D. Copying the directories $FWDIR/conf and $FWDIR/lib to another location.

Answer: A

Question: 31

You need to back up the routing, interface, and DNS configuration information from your R75 SecurePlatform Security Gateway. Which backup-and-restore solution do you use?

A. SecurePlatform back up utilities
B. Manual copies of the directory $FWDIR/conf
C. Database Revision Control
D. Commands upgrade_export and upgrade_import

Answer: A