Vendor: Checkpoint

Exam Code: 156-915.77

Exam Name: Check Point Certified Security Expert Update

Version: Demo

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.

Correct 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

Correct 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. Smart Provisioning
B. Smart Blade
C. Smart Dashboard
D. Smart LSM

Correct Answer: B

QUESTION 4
From the following output of cphaprob state, which Cluster XL mode is this?

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

Correct Answer: D

QUESTION 5
Which of the following is NOT a feature of Cluster XL?

A. Enhanced throughput in all Cluster XL 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

Correct 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

Correct 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%

Correct Answer: C

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 unload local

Correct Answer: D

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

Correct Answer: D

QUESTION 10
The process _____ compiles $FWDIR/conf/*.W files into machine language.

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

Correct 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

Correct 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 Smart Center.

Correct Answer: B

QUESTION 13
What process is responsible for transferring the policy file from Smart Center to the Gateway?

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

Correct 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

Correct Answer: D

QUESTION 15
Where do you define NAT properties so that NAT is performed either client side or server side?

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

Correct 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

Correct Answer: A

QUESTION 17
The process _____ is responsible for GUI Client communication with the Smart Center.

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

Correct Answer: B

QUESTION 18
The process _____ is responsible for Policy compilation.

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

Correct Answer: A

QUESTION 19
The process _____ is responsible for Management High Availability synchronization.

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

Correct Answer: B

QUESTION 20
_____ is the called process that starts when opening Smart View Tracker application.

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

Correct 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

Correct 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

Correct 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

Correct 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.

Correct 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.

Correct 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.

Correct Answer: D

QUESTION 27
A snapshot delivers a complete backup of Secure Platform. The resulting file can be stored on servers or as a local file in /var/CP snapshot/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.

Correct 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 Smart View 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.

Correct 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.

Correct Answer: B

QUESTION 30
Your primary Security Management Server runs on GAiA. What is the easiest way to back up your Security Gateway R76 configuration, including routing and network configuration files?

A. Using the native GAiA backup 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.

Correct Answer: A

QUESTION 31
You need to back up the routing, interface, and DNS configuration information from your R76 Secure Platform Security Gateway. Which backup-and-restore solution do you use?

A. Secure Platform back up utilities
B. Manual copies of the directory $FWDIR/conf
C. Database Revision Control
D. Commands upgrade export and upgrade import

Correct Answer: A

QUESTION 32
Which of the following methods will provide the most complete backup of an R76 configuration?

A. Database Revision Control
B. Policy Package Management
C. Copying the directories $FWDIR\conf and $CPDIR\conf to another server
D. upgrade export command

Correct Answer: D

QUESTION 33
Which of the following commands can provide the most complete restore of an R76 configuration?

A. upgrade import
B. fwm dbimport -p <export file>
C. cpconfig
D. cpinfo -recover

Correct Answer: A

QUESTION 34
When restoring R76 using the command upgrade import, which of the following items are NOT restored?

A. Global properties
B. Route tables
C. Licenses
D. SIC Certificates

Correct Answer: B

QUESTION 35
Your organization's disaster recovery plan needs an update to the backup and restore section to reap the benefits of the new distributed R76 installation. Your plan must meet the following required and desired objectives:

Required Objective: The Security Policy repository must be backed up no less frequently than every 24 hours.

Desired Objective: The R76 components that enforce the Security Policies should be backed up at least once a week.

Desired Objective: Back up R76 logs at least once a week.

Your disaster recovery plan is as follows:

- Use the utility `cron` to run the command `upgrade_export` each night on the Security Management Servers.
- Configure the organization's routine back up software to back up the files created by the command `upgrade_export`.
- Configure the SecurePlatform back up utility to back up the Security Gateways every Saturday night.
- Use the utility `cron` to run the command `upgrade_export` each Saturday night on the log servers.
- Configure an automatic, nightly `logswitch`.
- Configure the organization's routine back up software to back up the switched logs every night.

Upon evaluation, your plan:

A. Meets the required objective and only one desired objective
B. Meets the required objective and both desired objectives
C. Meets the required objective but does not meet either desired objective
D. Does not meet the required objective

Correct Answer: B

QUESTION 36
You are running a R76 Security Gateway on Secure Platform. In case of a hardware failure, you have a server with the exact same hardware and firewall version installed. What backup method could be used to quickly put the secondary firewall into production?

A. upgrade export
B. manual backup
C. snapshot
D. backup

Correct Answer: C

QUESTION 37
Before upgrading Secure Platform, you should create a backup. To save time, many administrators use the command backup. This creates a backup of the Check Point configuration as well as the system configuration.

An administrator has installed the latest HFA on the system for fixing traffic problems after creating a backup file. There is a mistake in the very complex static routing configuration. The Check Point configuration has not been changed. Can the administrator use a restore to fix the errors in static routing?

A. The restore is not possible because the backup file does not have the same build number (version).
B. The restore is done by selecting Snapshot Management from the Secure Platform boot menu.
C. The restore can be done easily by the command restore and selecting the appropriate backup file.

D. A back up cannot be restored, because the binary files are missing.

Correct Answer: C

QUESTION 38
You intend to upgrade a Check Point Gateway from R65 to R76. To avoid problems, you decide to back up the Gateway. Which approach allows the Gateway configuration to be completely backed up into a manageable size in the least amount of time?

A. snapshot
B. database revision
C. backup
D. upgrade export

Correct Answer: D

QUESTION 39
Your R76 enterprise Security Management Server is running abnormally on Windows 2008 Server. 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. Create a database revision control backup using the Smart Dashboard
2. Create a compressed archive of the *FWDIR*\ conf and »FWDiR8\lib directories and copy them to another networked machine.
3. Uninstall all R70 packages via Add/Remove Programs and reboot.
4. Install again as a primary Security Management Server using the R70 CD.
5. Reboot and restore the two archived directories over the top of the new installation, choosing to overwrite existing files.
B. 1. Download the latest upgrade export utility and run it from a c; \temp directory to export the configuration into a .tgz file
2. Skip any upgarde__verification warnings since you are not upgrading
3. Transfer the .tgz file to another networked machine
4. Download and run the cpclean utility and reboot
5. Use the R70 CD-ROM to select the uuarade import ootion to import the configuration
C. 1. Download the latest upqrade_expoct utility and run it from a \temp directory to export the configuration into a .tgz file
2. Perform any requested upgcade_veriJic«tion suggested steps
3. Uninstall all R70 packages via Add/Remove Programs and reboot
4. Use Smart Update to reinstall the Security Management Server and reboot
5. Transfer the tgz file back to the local \temp
6. Run upgrade__import to import the configuration
D. 1. Insert the F70 CD-ROM, and select the option to export the configuration using the latest upgrade utilities
2. Perform any requested upgrade verification suggested steps and re-export the configuration if needed
3. Save the export " tgz file to a local c: \temp directory
4. Uninstall all R70 packages via Add/Remove Programs and reboot
5. Install again using the R70 CD-ROM as a primary Security Management Server and reboot
6. Run upgrade import to import the configuration

Correct Answer: C

QUESTION 40
True or false? After creating a snapshot of a Windows 2003 SP2 Security Management Server, you can restore it on a Secure Platform R76 Security Management Server, except you must load interface information manually.

A. True, but only when the snapshot file is restored to a Secure Platform system running R76.20.
B. False, you cannot run the Check Point snapshot utility on a Windows gateway.

C. True, but only when the snapshot file is restored to a Secure Platform system running R76.10.
D. False, all configuration information conveys to the new system, including the interface configuration settings.

Correct Answer: B

QUESTION 41
Check Point recommends that you back up systems running Check Point products. Run your back ups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend before major changes, such as upgrades?

A. snapshot
B. upgrade export
C. backup
D. migrate export

Correct Answer: A

QUESTION 42
Check Point recommends that you back up systems running Check Point products. Run your back ups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend every couple of months, depending on how frequently you make changes to the network or policy?

A. backup
B. migrate export
C. upgrade export
D. snapshot

Correct Answer: A

QUESTION 43
Check Point recommends that you back up systems running Check Point products. Run your back ups during maintenance windows to limit disruptions to services, improve CPU usage, and simplify time allotment. Which back up method does Check Point recommend anytime outside a maintenance window?

A. backup
B. migrate export
C. backup export
D. snapshot

Correct Answer: B

QUESTION 44
Snapshot is available on which Security Management Server and Security Gateway platforms?

A. Solaris
B. Windows 2003 Server
C. Windows XP Server
D. Secure Platform

Correct Answer: D

QUESTION 45
The file snapshot generates is very large, and can only be restored to:

A. The device that created it, after it has been upgraded

B. Individual members of a cluster configuration
C. Windows Server class systems
D. A device having exactly the same Operating System as the device that created the file

Correct Answer: D

QUESTION 46
Restoring a snapshot-created file on one machine that was created on another requires which of the following to be the same on both machines?

A. Windows version, objects database, patch level, and interface configuration
B. Windows version, interface configuration, and patch level
C. State, Secure Platform version, and patch level
D. State, Secure Platform version, and objects database

Correct Answer: C

QUESTION 47
When restoring a Security Management Server from a backup file, the restore package can be retrieved from which source?

A. HTTP server, FTP server, or TFTP server
B. Disk, SCP server, or TFTP server
C. Local folder, TFTP server, or FTP server
D. Local folder, TFTP server, or Disk

Correct Answer: C

QUESTION 48
When upgrading Check Point products in a distributed environment, in which order should you upgrade these components?
1 GUI Client
2 Security Management Server
3 Security Gateway

A. 3, 2, 1
B. 1, 2, 3
C. 3, 1, 2
D. 2, 3, 1

Correct Answer: D

QUESTION 49
When using migrate to upgrade a Secure Management Server, which of the following is included in the migration?

A. Smart Event database
B. Smart Reporter database
C. classes. C file
D. System interface configuration

Correct Answer: C

QUESTION 50
Typically, when you upgrade the Security Management Server, you install and configure a fresh R76 installation on a new computer and then migrate the database from the original machine. When doing this, what is required of the two machines? They must both have the same:

A. Products installed.
B. Interfaces configured.
C. State.
D. Patch level.

Correct Answer: A

QUESTION 51
Typically, when you upgrade the Security Management Server, you install and configure a fresh R76 installation on a new computer and then migrate the database from the original machine.
Which of the following statements are TRUE?

A. Both machines must have the same number of interfaces installed and configured before migration can be attempted.
B. The new machine may not have more Check Point products installed than the original Security Management Server.
C. All product databases are included in the migration.
D. The Security Management Server on the new machine must be the same or greater than the version on the original machine.

Correct Answer: D

QUESTION 52
Typically, when you upgrade the Security Management Server, you install and configure a fresh R76 installation on a new computer and then migrate the database from the original machine. What is the correct order of the steps below to successfully complete this procedure?

1) Export databases from source.
2) Connect target to network.
3) Prepare the source machine for export.
4) Import databases to target.
5) Install new version on target.
6) Test target deployment.

A. 6, 5, 3, 1, 4, 2
B. 3, 1, 5, 4, 2, 6
C. 5, 2, 6, 3, 1, 4
D. 3, 5, 1, 4, 6, 2

Correct Answer: D

QUESTION 53
During a Security Management Server migrate export, the system:

A. Creates a backup file that includes the Smart Event database.
B. Creates a backup file that includes the Smart Reporter database.
C. Creates a backup archive for all the Check Point configuration settings.
D. Saves all system settings and Check Point product configuration settings to a file.

Correct Answer: C

QUESTION 54
If no flags are defined during a back up on the Security Management Server, where does the system store the *.tgz file?

A. /var/opt/backups
B. /var/backups
C. /var/CPbackup/backups

D. /var/tmp/backups

Correct Answer: C

QUESTION 55
Which is NOT a valid option when upgrading Cluster Deployments?

A. Full Connectivity Upgrade
B. Fast path Upgrade
C. Minimal Effort Upgrade
D. Zero Downtime

Correct Answer: B

QUESTION 56
In a zero downtime firewall cluster environment what command do you run to avoid switching problems around the cluster.

A. cphaconf set mc_relod
B. cphaconf set clear_subs
C. cphaconf set_ccp broadcast
D. cphaconf set_ccp multicast

Correct Answer: C

QUESTION 57
In a "zero downtime" scenario, which command do you run manually after all cluster members are upgraded?

A. cphaconf set_ccp broadcast
B. cphaconf set clear_subs
C. cphaconf set mc_relod
D. cphaconf set_ccp multicast

Correct Answer: D

QUESTION 58
Which command provides cluster upgrade status?

A. cphaprob status
B. cphaprob ldstat
C. cphaprob fcustat
D. cphaprob tablestat

Correct Answer: C

QUESTION 59
John is upgrading a cluster from NGX R65 to R76. John knows that you can verify the upgrade process using the pre-upgrade verifier tool. When John is running Pre-Upgrade Verification, he sees the warning message:

Title: Incompatible pattern.

What is happening?

A. R76 uses a new pattern matching engine. Incompatible patterns should be deleted before upgrade process to complete it successfully.
B. Pre-Upgrade Verification process detected a problem with actual configuration and upgrade will be

aborted.

C. Pre-Upgrade Verification tool only shows that message but it is only informational.
D. The actual configuration contains user defined patterns in IPS that are not supported in R76. If the patterns are not fixed after upgrade, they will not be used with R76 Security Gateways.

Correct Answer: D

QUESTION 60
Which command would you use to save the interface information before upgrading a GAiA Gateway?

A. netstat rn > [filename].txt
B. ipconfig a > [filename].txt
C. ifconfig > [filename].txt
D. cp /etc/sysconfig/network.C [location]

Correct Answer: C

QUESTION 61
Which command would you use to save the routing information before upgrading a Secure Platform Gateway?

A. cp /etc/sysconfig/network.C [location]
B. netstat rn > [filename].txt
C. ifconfig > [filename].txt
D. ipconfig a > [filename].txt

Correct Answer: A

QUESTION 62
Which command would you use to save the routing information before upgrading a Windows Gateway?

A. ipconfig a > [filename].txt
B. ifconfig > [filename].txt
C. cp /etc/sysconfig/network.C [location]
D. netstat rn > [filename].txt

Correct Answer: D

QUESTION 63
Which command would you use to save the interface information before upgrading a Windows Gateway?

A. cp /etc/sysconfig/network.C [location]
B. ipconfig a > [filename].txt
C. ifconfig > [filename].txt
D. netstat rn > [filename].txt

Correct Answer: B

QUESTION 64
When upgrading a cluster in Full Connectivity Mode, the first thing you must do is see if all cluster members have the same products installed. Which command should you run?

A. fw fcu
B. cphaprob fcustat
C. cpconfig
D. fw ctl conn a

Correct Answer: D

QUESTION 65
A Minimal Effort Upgrade of a cluster:

A. Is only supported in major releases (R70 to R71, R71 to R76).
B. Is not a valid upgrade method in R76.
C. Treats each individual cluster member as an individual gateway.
D. Upgrades all cluster members except one at the same time.

Correct Answer: C

QUESTION 66
A Zero Downtime Upgrade of a cluster:

A. Upgrades all cluster members except one at the same time.
B. Is only supported in major releases (R70 to R71, R71 to R76).
C. Treats each individual cluster member as an individual gateway.
D. Is not a valid upgrade method in R76.

Correct Answer: A

QUESTION 67
A Full Connectivity Upgrade of a cluster:

A. Treats each individual cluster member as an individual gateway.
B. Upgrades all cluster members except one at the same time.
C. Is only supported in minor version upgrades (R70 to R71, R71 to R76).
D. Is not a valid upgrade method in R76.

Correct Answer: C

QUESTION 68
A Fast Path Upgrade of a cluster:

A. Upgrades all cluster members except one at the same time.
B. Treats each individual cluster member as an individual gateway.
C. Is not a valid upgrade method in R76.
D. Is only supported in major releases (R70 to R71, R75 to R76).

Correct Answer: C

QUESTION 69
How does Check Point recommend that you secure the sync interface between gateways?

A. Configure the sync network to operate within the DMZ.
B. Secure each sync interface in a cluster with Endpoint.
C. Use a dedicated sync network.
D. Encrypt all sync traffic between cluster members.

Correct Answer: C

QUESTION 70
How would you set the debug buffer size to 1024?

A. Run fw ctl set buf 1024
B. Run fw ctl kdebug 1024

C. Run fw ctl debug -buf 1024
D. Run fw ctl set int print_cons 1024

Correct Answer: C

QUESTION 71
Steve is troubleshooting a connection problem with an internal application. If he knows the source IP address is 192.168.4.125, how could he filter this traffic?

A. Run fw monitor -e "accept dsrc=192.168.4.125;"
B. Run fw monitor -e "accept dst=192.168.4.125;"
C. Run fw monitor -e "accept ip=192.168.4.125;"
D. Run fw monitor -e "accept src=192.168.4.125;"

Correct Answer: D

QUESTION 72
Check Point support has asked Tony for a firewall capture of accepted packets. What would be the correct syntax to create a capture file to a filename called monitor. out?

A. Run fw monitor -e "accept;" -f monitor.out
B. Run fw monitor -e "accept;" -c monitor.out
C. Run fw monitor -e "accept;" -o monitor.out
D. Run fw monitor -e "accept;" -m monitor.out

Correct Answer: C

QUESTION 73
What is NOT a valid LDAP use in Check Point Smart Directory?

A. Retrieve gateway CRL's
B. External users management
C. Enforce user access to internal resources
D. Provide user authentication information for the Security Management Server

Correct Answer: C

QUESTION 74
There are several Smart Directory (LDAP) features that can be applied to further enhance Smart Directory (LDAP) functionality, which of the following is NOT one of those features?

A. High Availability, where user information can be duplicated across several servers
B. Support multiple Smart Directory (LDAP) servers on which many user databases are distributed
C. Encrypted or non-encrypted Smart Directory (LDAP) Connections usage
D. Support many Domains under the same account unit

Correct Answer: D

QUESTION 75
Choose the BEST sequence for configuring user management in Smart Dashboard, using an LDAP server.

A. Configure a workstation object for the LDAP server, configure a server object for the LDAP Account Unit, and enable LDAP in Global Properties.
B. Configure a server object for the LDAP Account Unit, and create an LDAP resource object.
C. Enable LDAP in Global Properties, configure a host-node object for the LDAP server, and configure a server object for the LDAP Account Unit.
D. Configure a server object for the LDAP Account Unit, enable LDAP in Global Properties, and create an

LDAP resource object.

Correct Answer: C

QUESTION 76
The User Directory Software Blade is used to integrate which of the following with a R76 Security Gateway?

A. LDAP server
B. RADIUS server
C. Account Management Client server
D. User Authority server

Correct Answer: A

QUESTION 77
Your users are defined in a Windows 2008 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 R76?

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

Correct Answer: A

QUESTION 78
Which of the following commands do you run on the AD server to identify the DN name before configuring LDAP integration with the Security Gateway?

A. query ldap name administrator
B. dsquery user name administrator
C. ldapquery name administrator
D. cpquery name administrator

Correct Answer: B

QUESTION 79
In Smart Directory, what is each LDAP server called?

A. Account Server
B. Account Unit
C. LDAP Server
D. LDAP Unit

Correct Answer: B

QUESTION 80
What is the default port number for standard TCP connections with the LDAP server?

A. 398
B. 636
C. 389
D. 363

Correct Answer: C

QUESTION 81

What is the default port number for Secure Sockets Layer connections with the LDAP Server?

A. 363
B. 389
C. 398
D. 636

Correct Answer: D

QUESTION 82
When defining an Organizational Unit, which of the following are NOT valid object categories?

A. Domains
B. Resources
C. Users
D. Services

Correct Answer: A

QUESTION 83
When defining Smart Directory for High Availability (HA), which of the following should you do?

A. Replicate the same information on multiple Active Directory servers.
B. Configure Secure Internal Communications with each server and fetch branches from each.
C. Configure a Smart Directory Cluster object.
D. Configure the Smart Directory as a single object using the LDAP cluster IP. Actual HA functionality is configured on the servers.

Correct Answer: A

QUESTION 84
The set of rules that governs the types of objects in the directory and their associated attributes is called the:

A. LDAP Policy
B. Schema
C. Access Control List
D. Smart Database

Correct Answer: B

QUESTION 85
When using Smart Dashboard to manage existing users in Smart Directory, when are the changes applied?

A. Instantaneously
B. At policy installation
C. Never, you cannot manage users through Smart Dashboard
D. At database synchronization

Correct Answer: A

QUESTION 86
Where multiple Smart Directory servers exist in an organization, a query from one of the clients for user information is made to the servers based on a priority. By what category can this priority be defined?

A. Gateway or Domain
B. Location or Account Unit

C. Location or Domain
D. Gateway or Account Unit

Correct Answer: D

QUESTION 87
Each entry in Smart Directory has a unique _____ ?

A. Distinguished Name
B. Organizational Unit
C. Port Number Association
D. Schema

Correct Answer: A

QUESTION 88
With the User Directory Software Blade, you can create R76 user definitions on a(n) _____ Server.

A. Secure ID
B. LDAP
C. NT Domain
D. Radius

Correct Answer: B

QUESTION 89
Which describes the function of the account unit?

A. An Account Unit is the Check Point account that Smart Directory uses to access an (LDAP) server
B. An Account Unit is a system account on the Check Point gateway that Smart Directory uses to access an (LDAP) server
C. An Account Unit is the administration account on the LDAP server that Smart Directory uses to access to (LDAP) server
D. An Account Unit is the interface which allows interaction between the Security Management server and Security Gateways, and the Smart Directory (LDAP) server.

Correct Answer: D

QUESTION 90
An organization may be distributed across several Smart Directory (LDAP) servers. What provision do you make to enable a Gateway to use all available resources? Each Smart Directory (LDAP) server must be:

A. a member in the LDAP group.
B. a member in a group that is associated with one Account Unit.
C. represented by a separate Account Unit.
D. represented by a separate Account Unit that is a member in the LDAP group.

Correct Answer: C

QUESTION 91
Which is NOT a method through which Identity Awareness receives its identities?

A. GPO
B. Captive Portal
C. AD Query
D. Identity Agent

Correct Answer: A

QUESTION 92
If using AD Query for seamless identity data reception from Microsoft Active Directory (AD), which of the following methods is NOT Check Point recommended?

A. Leveraging identity in Internet application control
B. Identity-based auditing and logging
C. Basic identity enforcement in the internal network
D. Identity-based enforcement for non-AD users (non-Windows and guest users)

Correct Answer: D

QUESTION 93
When using Captive Portal to send unidentified users to a Web portal for authentication, which of the following is NOT a recommended use for this method?

A. Identity-based enforcement for non-AD users (non-Windows and guest users)
B. For deployment of Identity Agents
C. Basic identity enforcement in the internal network
D. Leveraging identity in Internet application control

Correct Answer: C

QUESTION 94
Identity Agent is a lightweight endpoint agent that authenticates securely with Single Sign-On (SSO). Which of the following is NOT a recommended use for this method?

A. When accuracy in detecting identity is crucial
B. Identity based enforcement for non-AD users (non-Windows and guest users)
C. Protecting highly sensitive servers
D. Leveraging identity for Data Center protection

Correct Answer: B

QUESTION 95
Which of the following access options would you NOT use when configuring Captive Portal?

A. Through the Firewall policy
B. From the Internet
C. Through all interfaces
D. Through internal interfaces

Correct Answer: B

QUESTION 96
Where do you verify that Smart Directory is enabled?

A. Global properties > Authentication> Use Smart Directory(LDAP) for Security Gateways is checked
B. Gateway properties> Smart Directory (LDAP) > Use Smart Directory(LDAP) for Security Gateways is checked
C. Gateway properties > Authentication> Use Smart Directory(LDAP) for Security Gateways is checked
D. Global properties > Smart Directory (LDAP) > Use Smart Directory(LDAP) for Security Gateways is checked

Correct Answer: D

QUESTION 97
Remote clients are using IPSec VPN to authenticate via LDAP server to connect to the organization.

Which gateway process is responsible for the authentication?

A. vpnd
B. cpvpnd
C. fwm
D. fwd

Correct Answer: A

QUESTION 98
Remote clients are using SSL VPN to authenticate via LDAP server to connect to the organization. Which gateway process is responsible for the authentication?

A. vpnd
B. cpvpnd
C. fwm
D. fwd

Correct Answer: B

QUESTION 99
Which of the following is NOT a LDAP server option in Smart Directory?

A. Novell_DS
B. Netscape_DS
C. OPSEC_DS
D. Standard_DS

Correct Answer: D

QUESTION 100
An Account Unit is the interface between the _____ and the _____.

A. Users, Domain
B. Gateway, Resources
C. System, Database
D. Clients, Server

Correct Answer: D

QUESTION 101
Which of the following is a valid Active Directory designation for user John Doe in the Sales department of AcmeCorp.com?

A. Cn=john_doe,ou=Sales,ou=acmecorp,dc=com
B. Cn=john_doe,ou=Sales,ou=acme,ou=corp,dc=com
C. Cn=john_doe,dc=Sales,dc=acmecorp,dc=com
D. Cn=john_doe,ou=Sales,dc=acmecorp,dc=com

Correct Answer: D

QUESTION 102
Which of the following is a valid Active Directory designation for user Jane Doe in the MIS department of AcmeCorp.com?

A. Cn= jane_doe,ou=MIS,DC=acmecorp,dc=com
B. Cn= jane_doe,ou=MIS,cn=acmecorp,dc=com

C. Cn=jane_doe,ou=MIS,dc=acmecorp,dc=com
D. Cn= jane_doe,ou=MIS,cn=acme,cn=corp,dc=com

Correct Answer: C

QUESTION 103
Which utility or command is useful for debugging by capturing packet information, including verifying LDAP authentication?

A. fw monitor
B. ping
C. um_core enable
D. fw debug fwm

Correct Answer: A

QUESTION 104
You can NOT use Smart Dashboard's Smart Directory features to connect to the LDAP server.
What should you investigate?

1. Verify you have read-only permissions as administrator for the operating system.

2. Verify there are no restrictions blocking Smart Dashboard's User Manager from connecting to the LDAP server.

3. Check that the Login Distinguished Name configured has root (Administrator) permission (or at least write permission) in the access control configuration of the LDAP server.

A. 1 and 3
B. 2 and 3
C. 1 and 2
D. 1, 2, and 3

Correct Answer: B

QUESTION 105
If you are experiencing LDAP issues, which of the following should you check?

A. Secure Internal Communications (SIC)
B. Domain name resolution
C. Overlapping VPN Domains
D. Connectivity between the R76 Gateway and LDAP server

Correct Answer: D

QUESTION 106
How are cached usernames and passwords cleared from the memory of a R76 Security Gateway?

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

Correct Answer: D

QUESTION 107
When an Endpoint user is able to authenticate but receives a message from the client that it is unable to enforce the desktop policy, what is the most likely scenario?

A. The user's rights prevent access to the protected network.
B. A Desktop Policy is not configured.
C. The gateway could not locate the user in Smart Directory and is allowing the connection with limitations based on a generic profile.
D. The user is attempting to connect with the wrong Endpoint client.

Correct Answer: D

QUESTION 108
When using a template to define a Smart Directory, where should the user's password be defined? In the:

A. Template object
B. VPN Community object
C. User object
D. LDAP object

Correct Answer: C

QUESTION 109
When configuring an LDAP Group object, which option should you select if you want the gateway to reference the groups defined on the LDAP server for authentication purposes?

A. All Account-Unit's Users
B. Only Group in Branch
C. Group Agnostic
D. OU Accept and select appropriate domain

Correct Answer: B

QUESTION 110
When configuring an LDAP Group object, which option should you select if you do NOT want the gateway to reference the groups defined on the LDAP server for authentication purposes?

A. OU Accept and select appropriate domain
B. Only Sub Tree
C. Only Group in Branch
D. Group Agnostic

Correct Answer: B

QUESTION 111
When configuring an LDAP Group object, which option should you select if you want the gateway to reference the groups defined on the LDAP server for authentication purposes?

A. Only Group in Branch
B. Only Sub Tree
C. OU Auth and select Group Name
D. All Account-Unit's Users

Correct Answer: A

QUESTION 112
The process that performs the authentication for Smart Dashboard is:

A. fwm
B. vpnd
C. cvpnd

D. cpd

Correct Answer: A

QUESTION 113
The process that performs the authentication for Remote Access is:

A. cpd
B. vpnd
C. fwm
D. cvpnd

Correct Answer: B

QUESTION 114
The process that performs the authentication for SSL VPN Users is:

A. cvpnd
B. cpd
C. fwm
D. vpnd

Correct Answer: A

QUESTION 115
The process that performs the authentication for legacy session authentication is:

A. cvpnd
B. fwm
C. vpnd
D. fwssd

Correct Answer: D

QUESTION 116
While authorization for users managed by Smart Directory is performed by the gateway, the authentication is mostly performed by the infrastructure in which of the following?

A. ldapd
B. cpauth
C. cpShared
D. ldapauth

Correct Answer: B

QUESTION 117
When troubleshooting user authentication, you may see the following entries in a debug of the user authentication process. In which order are these messages likely to appear?

A. make_au, au_auth, au_fetchuser, au_auth_auth, cpLdapCheck, cpLdapGetUser
B. cpLdapGetUser, au_fetchuser, cpLdapCheck, make_au, au_auth, au_auth_auth
C. make_au, au_auth, au_fetchuser, cpLdapGetUser, cpLdapCheck, au_auth_auth
D. au_fetchuser, make_au, au_auth, cpLdapGetUser, au_auth_auth, cpLdapCheck

Correct Answer: C

QUESTION 118
Which of the following is NOT a Cluster XL mode?

A. Multicast
B. Legacy
C. Broadcast
D. New

Correct Answer: C

QUESTION 119
In an R76 Cluster, some features such as VPN only function properly when:

A. All cluster members have the same policy
B. All cluster members have the same Hot Fix Accumulator pack installed
C. All cluster members' clocks are synchronized
D. All cluster members have the same number of interfaces configured

Correct Answer: C

QUESTION 120
In Cluster XL R76; when configuring a cluster synchronization network on a VLAN interface what is the supported configuration?

A. It is supported on VLAN tag 4095
B. It is supported on VLAN tag 4096
C. It is supported on the lowest VLAN tag of the VLAN interface
D. It is not supported on a VLAN tag

Correct Answer: C

QUESTION 121
Which process is responsible for delta synchronization in Cluster XL?

A. fw kernel on the security gateway
B. fwd process on the security gateway
C. cpd process on the security gateway
D. Clustering process on the security gateway

Correct Answer: A

QUESTION 122
Which process is responsible for full synchronization in Cluster XL?

A. fwd on the Security Gateway
B. fw kernel on the Security Gateway
C. Clustering on the Security Gateway
D. cpd on the Security Gateway

Correct Answer: A

QUESTION 123
Which process is responsible for kernel table information sharing across all cluster members?

A. fwd daemon using an encrypted TCP connection
B. CPHA using an encrypted TCP connection
C. fw kernel using an encrypted TCP connection
D. cpd using an encrypted TCP connection

Correct Answer: A

QUESTION 124
By default, a standby Security Management Server is automatically synchronized by an active Security Management Server, when:

A. The user data base is installed.
B. The standby Security Management Server starts for the first time.
C. The Security Policy is installed.
D. The Security Policy is saved.

Correct Answer: C

QUESTION 125
The _____ Check Point Cluster XL mode must synchronize the physical interface IP and MAC addresses on all clustered interfaces.

A. New Mode HA
B. Pivot Mode Load Sharing
C. Multicast Mode Load Sharing
D. Legacy Mode HA

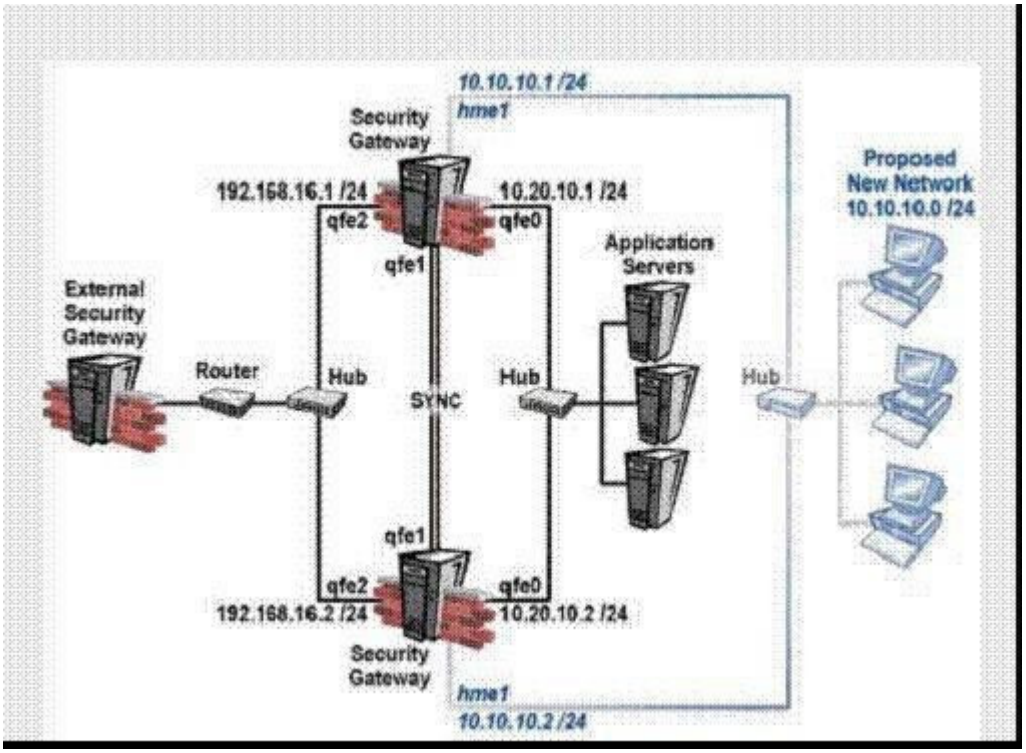
Correct Answer: D

QUESTION 126
_____ is a proprietary Check Point protocol. It is the basis for Check Point Cluster XL inter-module communication.

A. HA OPCODE
B. RDP
C. CKPP
D. CCP

Correct Answer: D

QUESTION 127
After you add new interfaces to a cluster, how can you check if the new interfaces and the associated virtual IP address are recognized by Cluster XL?



A. By running the command cphaprob state on both members
B. By running the command cpconfig on both members
C. By running the command cphaprob -I list on both members
D. By running the command cphaprob -a if on both members

Correct Answer: D

QUESTION 128
Which of the following is a supported Sticky Decision Function of Sticky Connections for Load Sharing?

A. Multi-connection support for VPN-1 cluster members
B. Support for all VPN deployments (except those with third-party VPN peers)
C. Support for Secure Client/Secure mote/SSL Network Extender encrypted connections
D. Support for Performance Pack acceleration

Correct Answer: C

QUESTION 129
Included in the customer's network are some firewall systems with the Performance Pack in use. The customer wishes to use these firewall systems in a cluster (Load Sharing mode). He is not sure if he can use the Sticky Decision Function in this cluster. Explain the situation to him.

A. Sticky Decision Function is not supported when employing either Performance Pack or a hardware-based accelerator card. Enabling the Sticky Decision Function disables these acceleration products.
B. Cluster XL always supports the Sticky Decision Function in the Load Sharing mode.
C. The customer can use the firewalls with Performance Pack inside the cluster, which should support the Sticky Decision Function. It is just necessary to enable the Sticky Decision Function in the Smart Dashboard cluster object in the Cluster XL page, Advanced Load Sharing Configuration window.
D. The customer can use the firewalls with Performance Pack inside the cluster, which should support the Sticky Decision Function. It is just necessary to configure it with the Cluster XL_SDF_enable command.

Correct Answer: A

QUESTION 130

A connection is said to be Sticky when:

A. The connection information sticks in the connection table even after the connection has ended.
B. A copy of each packet in the connection sticks in the connection table until a corresponding reply packet is received from the other side.
C. A connection is not terminated by either side by FIN or RST packet.
D. All the connection packets are handled, in either direction, by a single cluster member.

Correct Answer: D

QUESTION 131
How does a cluster member take over the VIP after a failover event?

A. Broadcast storm
B. iflist -renew
C. Ping the sync interface
D. Gratuitous ARP

Correct Answer: D

QUESTION 132
Check Point Clustering protocol, works on:

A. UDP 500
B. UDP 8116
C. TCP 8116
D. TCP 19864

Correct Answer: B

QUESTION 133
A customer is calling saying one member's status is Down. What will you check?

A. cphaprob list (verify what critical device is down)
B. fw ctl pstat (check sync)
C. fw ctl debug -m cluster + forward (forwarding layer debug)
D. tcpdump/snoop (CCP traffic)

Correct Answer: A

QUESTION 134
A customer calls saying that a Load Sharing cluster shows drops with the error First packet is not SYN. Complete the following sentence. I will recommend:

A. turning on SDF (Sticky Decision Function)
B. turning off SDF (Sticky Decision Function)
C. changing the load on each member
D. configuring flush and ack

Correct Answer: A

QUESTION 135
Which of the following commands can be used to troubleshoot Cluster XL sync issues?

A. fw debug cxl connections > file_name
B. fw tab -s -t connections > file_name
C. fw tab -u connections > file_name

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

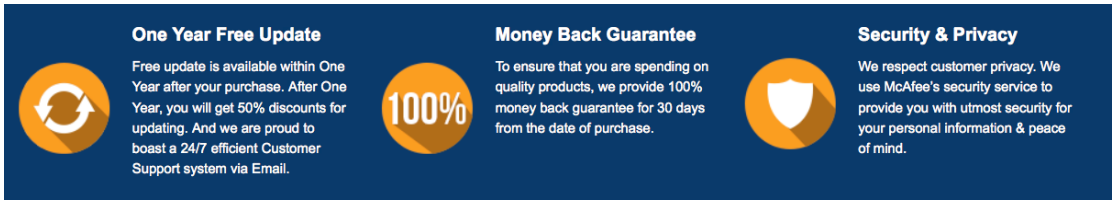
★ Average **99.9%** Success Rate

★ 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:



Guarantee & Policy | Privacy & Policy | Terms & Conditions