

Check-Point

Exam Questions 156-215.80

Check Point Certified Security Administrator



NEW QUESTION 1

- (Exam Topic 1)

What does the “unknown” SIC status shown on SmartConsole mean?

- A. The SMS can contact the Security Gateway but cannot establish Secure Internal Communication.
- B. SIC activation key requires a reset.
- C. The SIC activation key is not known by any administrator.
- D. There is no connection between the Security Gateway and SMS.

Answer: D

Explanation:

The most typical status is Communicating. Any other status indicates that the SIC communication is problematic. For example, if the SIC status is Unknown then there is no connection between the Gateway and the Security Management server. If the SIC status is Not Communicating, the Security Management server is able to contact the gateway, but SIC communication cannot be established.

NEW QUESTION 2

- (Exam Topic 1)

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Stateful Inspection
- C. Packet Filtering
- D. Application Layer Firewall

Answer: B

NEW QUESTION 3

- (Exam Topic 1)

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

Answer: B

Explanation:

To create a new permission profile:

In SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.

Click New Profile.

The New Profile window opens.

Enter a unique name for the profile.

Select a profile type:

Read/Write All - Administrators can make changes

Auditor (Read Only All) - Administrators can see information but cannot make changes

Customized - Configure custom settings

Click OK.

NEW QUESTION 4

- (Exam Topic 1)

Which of the following is TRUE regarding Gaia command line?

- A. Configuration changes should be done in mgmt_cli and use CLISH for monitoring, Expert mode is used only for OS level tasks.
- B. Configuration changes should be done in expert-mode and CLISH is used for monitoring.
- C. Configuration changes should be done in mgmt-cli and use expert-mode for OS-level tasks.
- D. All configuration changes should be made in CLISH and expert-mode should be used for OS-level tasks.

Answer: D

NEW QUESTION 5

- (Exam Topic 1)

Two administrators Dave and Jon both manage R80 Management as administrators for ABC Corp. Jon logged into the R80 Management and then shortly after Dave logged in to the same server. They are both in the Security Policies view. From the screenshots below, why does Dave not have the rule no.6 in his SmartConsole view even though Jon has it in his SmartConsole view?

- A. Jon is currently editing rule no.6 but has Published part of his changes.
- B. Dave is currently editing rule no.6 and has marked this rule for deletion.
- C. Dave is currently editing rule no.6 and has deleted it from his Rule Base.
- D. Jon is currently editing rule no.6 but has not yet Published his changes.

Answer: D

Explanation:

When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited. To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

NEW QUESTION 6

- (Exam Topic 1)

When you upload a package or license to the appropriate repository in SmartUpdate, where is the package or license stored

- A. Security Gateway
- B. Check Point user center
- C. Security Management Server
- D. SmartConsole installed device

Answer: C

Explanation:

SmartUpdate installs two repositories on the Security Management server:

License & Contract Repository, which is stored on all platforms in the directory \$FWDIR\conf\.

Package Repository, which is stored:

on Windows machines in C:\SUroot.

on UNIX machines in /var/suroot.

The Package Repository requires a separate license, in addition to the license for the Security Management server. This license should stipulate the number of nodes that can be managed in the Package Repository.

NEW QUESTION 7

- (Exam Topic 1)

Vanessa is firewall administrator in her company; her company is using Check Point firewalls on central and remote locations, which are managed centrally by R80 Security Management Server. One central location has an installed R77.30 Gateway on Open server. Remote location is using Check Point UTM-1 570 series appliance with R71. Which encryption is used in Secure Internal Communication (SIC) between central management and firewall on each location?

- A. On central firewall AES128 encryption is used for SIC, on Remote firewall 3DES encryption is used for SIC.
- B. On both firewalls, the same encryption is used for SI
- C. This is AES-GCM-256.
- D. The Firewall Administrator can choose which encryption suite will be used by SIC.
- E. On central firewall AES256 encryption is used for SIC, on Remote firewall AES128 encryption is used for SIC.

Answer: A

Explanation:

Gateways above R71 use AES128 for SIC. If one of the gateways is R71 or below, the gateways use 3DES.

NEW QUESTION 8

- (Exam Topic 1)

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

- A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
- B. Create a separate Security Policy package for each remote Security Gateway.
- C. Create network object that restrict all applicable rules to only certain networks.
- D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

Review the following screenshot and select the BEST answer.

- A. Data Center Layer is an inline layer in the Access Control Policy.
- B. By default all layers are shared with all policies.
- C. If a connection is dropped in Network Layer, it will not be matched against the rules in Data Center Layer.
- D. If a connection is accepted in Network-layer, it will not be matched against the rules in Data Center Layer.

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

Which type of the Check Point license ties the package license to the IP address of the Security Management Server?

- A. Local
- B. Central
- C. Corporate
- D. Formal

Answer: B

NEW QUESTION 10

- (Exam Topic 1)

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

- A. remove database lock
- B. The database feature has one command lock database override.
- C. override database lock
- D. The database feature has two commands: lock database override and unlock databas
- E. Both will work.

Answer: D

Explanation:

Use the database feature to obtain the configuration lock. The database feature has two commands:

lock database [override].
unlock database

The commands do the same thing: obtain the configuration lock from another administrator.

NEW QUESTION 11

- (Exam Topic 1)

Which application should you use to install a contract file?

- A. SmartView Monitor
- B. WebUI
- C. SmartUpdate
- D. SmartProvisioning

Answer: C

Explanation:

Using SmartUpdate: If you already use an NGX R65 (or higher) Security Management / Provider-1 /

Multi-Domain Management Server, SmartUpdate allows you to import the service contract file that you have downloaded in Step #3.

Open SmartUpdate and from the Launch Menu select 'Licenses & Contracts' -> 'Update Contracts' -> 'From File...' and provide the path to the file you have downloaded in Step #3:

Note: If SmartUpdate is connected to the Internet, you can download the service contract file directly from the UserCenter without going through the download and import steps.

NEW QUESTION 12

- (Exam Topic 1)

Choose the Best place to find a Security Management Server backup file named backup_fw, on a Check Point Appliance.

- A. /var/log/Cpbackup/backups/backup/backup_fw.tgs
- B. /var/log/Cpbackup/backups/backup/backup_fw.tar
- C. /var/log/Cpbackup/backups/backups/backup_fw.tar
- D. /var/log/Cpbackup/backups/backup_fw.tgz

Answer: D

Explanation:

Gaia's Backup feature allows backing up the configuration of the Gaia OS and of the Security Management server database, or restoring a previously saved configuration. The configuration is saved to a .tgz file in the following directory:

Gaia OS Version Hardware
Local Directory R75.40 - R77.20
Check Point appliances

/var/log/CPbackup/backups/ Open Server
/var/CPbackup/backups/ R77.30
Check Point appliances
/var/log/CPbackup/backups/ Open Server

NEW QUESTION 16

- (Exam Topic 1)

Fill in the blank: With the User Directory Software Blade, you can create R80 user definitions on a(an) _____ Server.

- A. NT domain
- B. SMTP
- C. LDAP
- D. SecurID

Answer: C

NEW QUESTION 18

- (Exam Topic 1)

Which utility shows the security gateway general system information statistics like operating system information and resource usage, and individual software blade statistics of VPN, Identity Awareness and DLP?

- A. cpconfig
- B. fw ctl pstat
- C. cpview
- D. fw ctl multik stat

Answer: C

Explanation:

CPView Utility is a text based built-in utility that can be run ('cpview' command) on Security Gateway / Security Management Server / Multi-Domain Security Management Server. CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Gateway). The data is continuously updated in easy to access views.

NEW QUESTION 19

- (Exam Topic 1)

Fill in the blank: The _____ is used to obtain identification and security information about network users.

- A. User Directory
- B. User server
- C. UserCheck
- D. User index

Answer: A

NEW QUESTION 21

- (Exam Topic 1)

Fill in the blanks: VPN gateways authenticate using _____ and _____.

- A. Passwords; tokens
- B. Certificates; pre-shared secrets
- C. Certificates; passwords
- D. Tokens; pre-shared secrets

Answer: B

Explanation:

VPN gateways authenticate using Digital Certificates and Pre-shared secrets.

NEW QUESTION 26

- (Exam Topic 1)

Fill in the blank: The command _____ provides the most complete restoration of a R80 configuration.

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

Answer: A

Explanation:

(Should be "migrate import")

"migrate import" Restores backed up configuration for R80 version, in previous versions the command was " upgrade_import ".

NEW QUESTION 30

- (Exam Topic 1)

Which one of the following is the preferred licensing model? Select the Best answer.

- A. Local licensing because it ties the package license to the IP-address of the gateway and has no dependency of the Security Management Server.
- B. Central licensing because it ties the package license to the IP-address of the Security Management Server and has no dependency of the gateway.
- C. Local licensing because it ties the package license to the MAC-address of the gateway management interface and has no Security Management Server dependency.
- D. Central licensing because it ties the package license to the MAC-address of the Security Management Server Mgmt-interface and has no dependency of the gateway.

Answer: B

Explanation:

Central License

A Central License is a license attached to the Security Management server IP address, rather than the gateway IP address. The benefits of a Central License are:
Only one IP address is needed for all licenses.

A license can be taken from one gateway and given to another.

The new license remains valid when changing the gateway IP address. There is no need to create and install a new license.

NEW QUESTION 32

- (Exam Topic 1)

Fill in the blank: RADIUS protocol uses _____ to communicate with the gateway.

- A. UDP
- B. TDP
- C. CCP
- D. HTTP

Answer: A

Explanation:

Parameters:

NEW QUESTION 34

- (Exam Topic 1)

In the Check Point three-tiered architecture, which of the following is NOT a function of the Security Management Server (Security Management Server)?

- A. Display policies and logs on the administrator's workstation.
- B. Verify and compile Security Policies.
- C. Processing and sending alerts such as SNMP traps and email notifications.
- D. Store firewall logs to hard drive storage.

Answer: A

NEW QUESTION 38

- (Exam Topic 1)

Which options are given on features, when editing a Role on Gaia Platform?

- A. Read/Write, Read Only
- B. Read/Write, Read only, None
- C. Read/Write, None
- D. Read Only, None

Answer: B

Explanation:

Roles

Role-based administration (RBA) lets you create administrative roles for users. With RBA, an administrator can allow Gaia users to access specified features by including those features in a role and assigning that role to users. Each role can include a combination of administrative (read/write) access to some features, monitoring (readonly) access to other features, and no access to other features.

You can also specify which access mechanisms (WebUI or the CLI) are available to the user.

Note - When users log in to the WebUI, they see only those features that they have read-only or read/write access to. If they have read-only access to a feature, they can see the settings pages, but cannot change the settings.

Gaia includes these predefined roles:

You cannot delete or change the predefined roles.

Note - Do not define a new user for external users. An external user is one that is defined on an authentication server (such as RADIUS or TACACS) and not on the local Gaia system.

NEW QUESTION 39

- (Exam Topic 1)

With which command can you view the running configuration of Gaia-based system.

- A. show conf-active
- B. show configuration active
- C. show configuration
- D. show running-configuration

Answer: C

NEW QUESTION 44

- (Exam Topic 1)

Where can you trigger a failover of the cluster members?

Log in to Security Gateway CLI and run command clusterXL_admin down.

In SmartView Monitor right-click the Security Gateway member and select Cluster member stop. Log into Security Gateway CLI and run command cphaprob down.

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

Answer: C

Explanation:

How to Initiate Failover

NEW QUESTION 48

- (Exam Topic 1)

What is NOT an advantage of Packet Filtering?

- A. Low Security and No Screening above Network Layer
- B. Application Independence
- C. High Performance
- D. Scalability

Answer: A

Explanation:

Packet Filter Advantages and Disadvantages

NEW QUESTION 50

- (Exam Topic 1)

Fill in the blank: Each cluster has _____ interfaces.

- A. Five
- B. Two
- C. Three
- D. Four

Answer: C

Explanation:

Each cluster member has three interfaces: one external interface, one internal interface, and one for synchronization. Cluster member interfaces facing in each

direction are connected via a switch, router, or VLAN switch.

NEW QUESTION 52

- (Exam Topic 1)

To optimize Rule Base efficiency, the most hit rules should be where?

- A. Removed from the Rule Base.
- B. Towards the middle of the Rule Base.
- C. Towards the top of the Rule Base.
- D. Towards the bottom of the Rule Base.

Answer: C

Explanation:

It is logical that if lesser rules are checked for the matched rule to be found the lesser CPU cycles the device is using. Checkpoint match a session from the first rule on top till the last on the bottom.

NEW QUESTION 55

- (Exam Topic 1)

Fill in the blank: The R80 feature _____ permits blocking specific IP addresses for a specified time period.

- A. Block Port Overflow
- B. Local Interface Spoofing
- C. Suspicious Activity Monitoring
- D. Adaptive Threat Prevention

Answer: C

Explanation:

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation

NEW QUESTION 58

- (Exam Topic 1)

You are unable to login to SmartDashboard. You log into the management server and run #cpwd_admin list with the following output:

What reason could possibly BEST explain why you are unable to connect to SmartDashboard?

- A. CDP is down
- B. SVR is down
- C. FWM is down
- D. CPSM is down

Answer: C

Explanation:

The correct answer would be FWM (is the process making available communication between SmartConsole applications and Security Management Server.).

STATE is T (Terminate = Down)

Symptoms

SmartDashboard fails to connect to the Security Management server.

Verify if the FWM process is running. To do this, run the command:

```
[Expert@HostName:0]# ps -aux | grep fwm
```

If the FWM process is not running, then try force-starting the process with the following command: [Expert@HostName:0]# cpwd_admin start -name FWM -path "\$FWDIR/bin/fwm" -command "fwm" [Expert@HostName:0]# ps -aux | grep fwm

```
[Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"
```

NEW QUESTION 60

- (Exam Topic 1)

What is the default time length that Hit Count Data is kept?

- A. 3 month
- B. 4 weeks
- C. 12 months
- D. 6 months

Answer: A

Explanation:

Keep Hit Count data up to - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.

NEW QUESTION 63

- (Exam Topic 1)

Examine the following Rule Base.

What can we infer about the recent changes made to the Rule Base?

- A. Rule 7 was created by the 'admin' administrator in the current session
- B. 8 changes have been made by administrators since the last policy installation
- C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator
- D. Rule 1 and object webserver are locked by another administrator

Answer: D

Explanation:

On top of the print screen there is a number "8" which consists for the number of changes made and not saved. Session Management Toolbar (top of SmartConsole)

NEW QUESTION 67

- (Exam Topic 2)

What is the potential downside or drawback to choosing the Standalone deployment option instead of the Distributed deployment option?

- A. degrades performance as the Security Policy grows in size
- B. requires additional Check Point appliances
- C. requires additional software subscription
- D. increases cost

Answer: A

NEW QUESTION 72

- (Exam Topic 2)

Which Check Point software blade provides protection from zero-day and undiscovered threats?

- A. Firewall
- B. Threat Emulation
- C. Application Control
- D. Threat Extraction

Answer: D

Explanation:

SandBlast Threat Emulation

As part of the Next Generation Threat Extraction software bundle (NGTX), the SandBlast Threat Emulation capability prevents infections from undiscovered exploits zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network.

NEW QUESTION 73

- (Exam Topic 2)

To install a brand new Check Point Cluster, the MegaCorp IT department bought 1 Smart-1 and 2 Security Gateway Appliances to run a cluster. Which type of cluster is it?

- A. Full HA Cluster
- B. High Availability
- C. Standalone
- D. Distributed

Answer: B

NEW QUESTION 74

- (Exam Topic 2)

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.

Answer: A

NEW QUESTION 79

- (Exam Topic 2)

You are the Security Administrator for MegaCorp. In order to see how efficient your firewall Rule Base is, you would like to see how many 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 directl
- E. You can open SmartDashboard and select UserDefined in the Track column
- F. Afterwards, you need to create your own program with an external counter.

Answer: C

NEW QUESTION 84

- (Exam Topic 2)

Fill in the blanks: The Application Layer Firewalls inspect traffic through the ____ layer(s) of the TCP/IP model and up to and including the ____ layer.

- A. Lower; Application
- B. First two; Internet
- C. First two; Transport
- D. Upper; Application

Answer: A

NEW QUESTION 87

- (Exam Topic 2)

Why would an administrator see the message below?

- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- D. A new Policy Package created on the Gateway and transferred to the management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 90

- (Exam Topic 2)

What does it mean if Bob gets this result on an object search? Refer to the image below. Choose the BEST answer.

- A. Search detailed is missing the subnet mask.
- B. There is no object on the database with that name or that IP address.
- C. There is no object on the database with that IP address.
- D. Object does not have a NAT IP address.

Answer: B

NEW QUESTION 95

- (Exam Topic 2)

Which of the following is NOT a back up method?

- A. Save backup
- B. System backup
- C. snapshot
- D. Migrate

Answer: A

Explanation:

The built-in Gaia backup procedures:

Snapshot Management

System Backup (and System Restore)

Save/Show Configuration (and Load Configuration)

Check Point provides three different procedures for backing up (and restoring) the operating system and networking parameters on your appliances.

Snapshot (Revert)

Backup (Restore)

upgrade_export (Migrate) References:

NEW QUESTION 100

- (Exam Topic 2)

You want to define a selected administrator's permission to edit a layer. However, when you click the + sign in the "Select additional profile that will be able edit this layer" you do not see anything. What is the most likely cause of this problem? Select the BEST answer.

- A. "Edit layers by Software Blades" is unselected in the Permission Profile
- B. There are no permission profiles available and you need to create one first.
- C. All permission profiles are in use.
- D. "Edit layers by selected profiles in a layer editor" is unselected in the Permission profile.

Answer: B

NEW QUESTION 104

- (Exam Topic 2)

Which of these components does NOT require a Security Gateway R77 license?

- A. Security Management Server
- B. Check Point Gateway
- C. SmartConsole
- D. SmartUpdate upgrading/patching

Answer: C

NEW QUESTION 107

- (Exam Topic 2)

What action can be performed from SmartUpdate R77?

- A. upgrade_export
- B. fw stat -1
- C. cpinfo
- D. remote_uninstall_verifier

Answer: C

NEW QUESTION 111

- (Exam Topic 2)

Choose what BEST describes a Session.

- A. Starts when an Administrator publishes all the changes made on SmartConsole.
- B. Starts when an Administrator logs in to the Security Management Server through SmartConsole and ends when it is published.
- C. Sessions ends when policy is pushed to the Security Gateway.
- D. Sessions locks the policy package for editing.

Answer: B

Explanation:

Administrator Collaboration

More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

When an administrator logs in to the Security Management Server through SmartConsole, a new editing session starts. The changes that the administrator makes during the session are only available to that administrator. Other administrators see a lock icon on object and rules that are being edited.

To make changes available to all administrators, and to unlock the objects and rules that are being edited, the administrator must publish the session.

NEW QUESTION 115

- (Exam Topic 2)

If there is an Accept Implied Policy set to "First", what is the reason Jorge cannot see any logs?

- A. Log Implied Rule was not selected on Global Properties.
- B. Log Implied Rule was not set correctly on the track column on the rules base.
- C. Track log column is set to none.
- D. Track log column is set to Log instead of Full Log.

Answer: A

Explanation:

Implied Rules are configured only on Global Properties.

NEW QUESTION 116

- (Exam Topic 2)

Fill in the blanks: A High Availability deployment is referred to as a ____ cluster and a Load Sharing deployment is referred to as a ____ cluster.

- A. Standby/standby; active/active
- B. Active/active; standby/standby
- C. Active/active; active/standby;
- D. Active/standby; active/active

Answer: D

Explanation:

In a High Availability cluster, only one member is active (Active/Standby operation).

ClusterXL Load Sharing distributes traffic within a cluster so that the total throughput of multiple members is increased. In Load Sharing configurations, all functioning members in the cluster are active, and handle network traffic (Active/Active operation).

NEW QUESTION 121

- (Exam Topic 2)

Fill in the blanks: A security Policy is created in _____, stored in the _____, and Distributed to the various _____.

- A. Rule base, Security Management Server, Security Gateways
- B. SmartConsole, Security Gateway, Security Management Servers
- C. SmartConsole, Security Management Server, Security Gateways
- D. The Check Point database, SmartConsole, Security Gateways

Answer: C

NEW QUESTION 122

- (Exam Topic 2)

Which directory holds the SmartLog index files by default?

- A. \$SMARTLOGDIR/data
- B. \$SMARTLOG/dir
- C. \$FWDIR/smartlog
- D. \$FWDIR/log

Answer: A

NEW QUESTION 124

- (Exam Topic 2)

Study the Rule base and Client Authentication Action properties screen.

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

- A. user is prompted for authentication by the Security Gateways 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.

Answer: C

NEW QUESTION 128

- (Exam Topic 2)

After the initial installation the First Time Configuration Wizard should be run. Select the BEST answer.

- A. First Time Configuration Wizard can be run from the Unified SmartConsole.
- B. First Time Configuration Wizard can be run from the command line or from the WebUI.
- C. First time Configuration Wizard can only be run from the WebUI.
- D. Connection to the internet is required before running the First Time Configuration wizard.

Answer: B

Explanation:

Check Point Security Gateway and Check Point Security Management require running the First Time Configuration Wizard in order to be configured correctly. The First Time Configuration Wizard is available in Gaia Portal and also through CLI.

To invoke the First Time Configuration Wizard through CLI, run the config_system command from the Exp shell.

NEW QUESTION 132

- (Exam Topic 2)

Fill in the blank: Once a license is activated, a _____ should be installed.

- A. License Management file
- B. Security Gateway Contract file
- C. Service Contract file
- D. License Contract file

Answer: C

Explanation:

Service Contract File

Following the activation of the license, a Service Contract File should be installed. This file contains important information about all subscriptions purchased for a specific device and is installed via SmartUpdate. A detailed Explanation: of the Service Contract File can be found in sk33089.

NEW QUESTION 134

- (Exam Topic 2)

You installed Security Management Server on a computer using GAiA in the MegaCorp home office. You use IP address 10.1.1.1. You also installed the Security Gateway on a second GAiA computer, which you plan to ship to another Administrator at a MegaCorp hub office. What is the correct order for pushing SIC certificates to the Gateway before shipping it?

1. Run cpconfig on the Gateway, select Secure Internal Communication, enter the activation key, and reconfirm.
2. Initialize Internal Certificate Authority (ICA) on the Security Management Server.
3. Configure the Gateway object with the host name and IP addresses for the remote site.
4. Click the Communication button in the Gateway object's General screen, enter the activation key, and click Initialize and OK.
5. Install the Security Policy.

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

Answer: B

NEW QUESTION 135

- (Exam Topic 2)

Choose what BEST describes users on Gaia Platform.

- A. There is one default user that cannot be deleted.
- B. There are two default users and one cannot be deleted.
- C. There is one default user that can be deleted.
- D. There are two default users that cannot be deleted and one SmartConsole Administrator.

Answer: B

Explanation:

These users are created by default and cannot be deleted:

admin — Has full read/write capabilities for all Gaia features, from the WebUI and the CLI. This user has a User ID of 0, and therefore has all of the privileges of a root user.

monitor — Has read-only capabilities for all features in the WebUI and the CLI, and can change its own password. You must give a password for this user before the account can be used.

NEW QUESTION 137

- (Exam Topic 2)

Administrator wishes to update IPS from SmartConsole by clicking on the option "update now" under the IPS tab. Which device requires internet access for the update to work?

- A. Security Gateway
- B. Device where SmartConsole is installed
- C. SMS
- D. SmartEvent

Answer: B

Explanation:

Updating IPS Manually

You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website. You can only manually update IPS if a proxy is defined in Internet Explorer settings.

To obtain updates of all the latest protections from the IPS website:

Configure the settings for the proxy server in Internet Explorer.

In Microsoft Internet Explorer, open Tools > Internet Options > Connections tab > LAN Settings.

The LAN Settings window opens.

Select Use a proxy server for your LAN.

Configure the IP address and port number for the proxy server.

Click OK.

The settings for the Internet Explorer proxy server are configured.

In the IPS tab, select Download Updates

and click Update Now.

NEW QUESTION 140

- (Exam Topic 2)

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

Answer: A

NEW QUESTION 145

- (Exam Topic 2)

There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW_A and FW_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW_A is configured to have higher priority than FW_B. FW_A was active and processing the traffic in the morning. FW_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW_B became active. After an hour, FW_A's interface issues were resolved and it became operational. When it re-joins the cluster, will it become active automatically?

- A. No, since “maintain current active cluster member” option on the cluster object properties is enabled by default
- B. No, since “maintain current active cluster member” option is enabled by default on the Global Properties
- C. Yes, since “Switch to higher priority cluster member” option on the cluster object properties is enabled by default
- D. Yes, since “Switch to higher priority cluster member” option is enabled by default on the Global Properties

Answer: A

Explanation:

What Happens When a Security Gateway Recovers?

In a Load Sharing configuration, when the failed Security Gateway in a cluster recovers, all connections are redistributed among all active members. High Availability and Load Sharing in ClusterXL ClusterXL Administration Guide R77 Versions | 31 In a High Availability configuration, when the failed Security Gateway in a cluster recovers, the recovery method depends on the configured cluster setting. The options are:

- Maintain Current Active Security Gateway means that if one member passes on control to a lower priority member, control will be returned to the higher priority member only if the lower priority member fails. This mode is recommended if all members are equally capable of processing traffic, in order to minimize the number of failover events.
- Switch to Higher Priority Security Gateway means that if the lower priority member has control and the higher priority member is restored, then control will be returned to the higher priority member. This mode is recommended if one member is better equipped for handling connections, so it will be the default Security Gateway.

NEW QUESTION 150

- (Exam Topic 2)

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

Answer: B

Explanation:

This chapter gives an introduction to the Gaia command line interface (CLI). The default shell of the CLI is called clish.

NEW QUESTION 154

- (Exam Topic 2)

Which policy type is used to enforce bandwidth and traffic control rules?

- A. Threat Emulation
- B. Access Control
- C. QoS
- D. Threat Prevention

Answer: C

Explanation:

Check Point's QoS Solution

QoS is a policy-based QoS management solution from Check Point Software Technologies Ltd., satisfies your needs for a bandwidth management solution. QoS is a unique, software-only based application that manages traffic end-to-end across networks, by distributing enforcement throughout network hardware and software.

NEW QUESTION 157

- (Exam Topic 2)

What happens if the identity of a user is known?

- A. If the user credentials do not match an Access Role, the system displays the Captive Portal.
- 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 traffic is automatically dropped.
- D. If the user credentials match an Access Role, the rule is applied and traffic is accepted or dropped based on the defined action.

Answer: D

NEW QUESTION 160

- (Exam Topic 2)

Fill in the blank: RADIUS Accounting gets _____ data from requests generated by the accounting client

- A. Destination
- B. Identity
- C. Payload
- D. Location

Answer: B

Explanation:

How RADIUS Accounting Works with Identity Awareness

RADIUS Accounting gets identity data from RADIUS Accounting Requests generated by the RADIUS accounting client.

NEW QUESTION 162

- (Exam Topic 2)
The Captive Portal tool:

- A. Acquires identities from unidentified users.
- B. Is only used for guest user authentication.
- C. Allows access to users already identified.
- D. Is deployed from the Identity Awareness page in the Global Properties settings.

Answer: A

NEW QUESTION 164

- (Exam Topic 2)
Message digests use which of the following?

- A. DES and RC4
- B. IDEA and RC4
- C. SSL and MD4
- D. SHA-1 and MD5

Answer: D

NEW QUESTION 169

- (Exam Topic 2)
Which authentication scheme requires a user to possess a token?

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

Answer: B

Explanation:

SecurID
SecurID requires users to both possess a token authenticator and to supply a PIN or password References:

NEW QUESTION 172

- (Exam Topic 2)
Fill in the blank: When LDAP is integrated with Check Point Security Management, it is then referred to as _____

- A. UserCheck
- B. User Directory
- C. User Administration
- D. User Center

Answer: B

Explanation:

Check Point User Directory integrates LDAP, and other external user management technologies, with the Check Point solution. If you have a large user count, we recommend that you use an external user management database such as LDAP for enhanced Security Management Server performance.

NEW QUESTION 173

- (Exam Topic 2)
You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?

- A. The POP3 rule is disabled.
- B. POP3 is accepted in Global Properties.
- C. The POP3 rule is hidden.
- D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.

Answer: C

NEW QUESTION 174

- (Exam Topic 2)
The fw monitor utility is used to troubleshoot which of the following problems?

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

Answer: B

NEW QUESTION 177

- (Exam Topic 2)

When using LDAP as an authentication method for Identity Awareness, the query:

- A. Requires client and server side software.
- B. Prompts the user to enter credentials.
- C. Requires administrators to specifically allow LDAP traffic to and from the LDAP Server and the Security Gateway.
- D. Is transparent, requiring no client or server side software, or client intervention.

Answer: D

NEW QUESTION 181

- (Exam Topic 2)

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.

Answer: C

NEW QUESTION 186

- (Exam Topic 2)

You are going to upgrade from R77 to R80. Before the upgrade, you want to back up the system so that, if there are any problems, you can easily restore to the old version with all configuration and management files intact. What is the BEST backup method in this scenario?

- A. backup
- B. Database Revision
- C. snapshot
- D. migrate export

Answer: C

Explanation:

2. Snapshot Management

The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system.

Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.

The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

NEW QUESTION 187

- (Exam Topic 2)

R80 Security Management Server can be installed on which of the following operating systems?

- A. Gaia only
- B. Gaia, SPLAT, Windows Server only
- C. Gaia, SPLAT, Windows Server and IPSO only
- D. Gaia and SPLAT only

Answer: A

Explanation:

R80 can be installed only on GAIA OS.

Supported Check Point Installations All R80 servers are supported on the Gaia Operating System:

- Security Management Server
- Multi-Domain Security Management Server
- Log Server
- Multi-Domain Log Server
- SmartEvent Server

NEW QUESTION 191

- (Exam Topic 2)

Jack works for a managed service provider and he has been tasked to create 17 new policies for several new customers. He does not have much time. What is the BEST way to do this with R80 security management?

- A. Create a text-file with mgmt_cli script that creates all objects and policie
- B. Open the file in SmartConsole Command Line to run it.
- C. Create a text-file with Gaia CLI -commands in order to create all objects and policie
- D. Run the file in CLISH with command load configuration.
- E. Create a text-file with DBEDIT script that creates all objects and policie
- F. Run the file in the command line of the management server using command dbedit -f.
- G. Use Object Explorer in SmartConsole to create the objects and Manage Policies from the menu to create the policies.

Answer: A

Explanation:

Did you know: mgmt_cli can accept csv files as inputs using the --batch option.

The first row should contain the argument names and the rows below it should hold the values for these parameters.

So an equivalent solution to the powershell script could look like this:

data.csv:

```
mgmt_cli add host --batch data.csv -u <username> -p <password> -m <management server>
```

This can work with any type of command not just "add host" : simply replace the column names with the ones relevant to the command you need.

NEW QUESTION 192

- (Exam Topic 2)

The organization's security manager wishes to back up just the Gaia operating system parameters. Which command can be used to back up only Gaia operating system parameters like interface details, Static routes and Proxy ARP entries?

- A. show configuration
- B. backup
- C. migrate export
- D. upgrade export

Answer: B

Explanation:

3. System Backup (and System Restore)

System Backup can be used to backup current system configuration. A backup creates a compressed file that contains the Check Point configuration including the networking and operating system parameters, such as routing and interface configuration etc., but unlike a snapshot, it does not include the operating system, product binaries, and hotfixes.

NEW QUESTION 197

- (Exam Topic 3)

The Firewall kernel is replicated multiple times, therefore:

- A. The Firewall kernel only touches the packet if the connection is accelerated
- B. The Firewall can run different policies per core
- C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
- D. The Firewall can run the same policy on all cores

Answer: D

NEW QUESTION 200

- (Exam Topic 3)

Which is the correct order of a log flow processed by SmartEvent components:

- A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
- B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
- C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
- D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

NEW QUESTION 202

- (Exam Topic 3)

According to Check Point Best Practice, when adding a 3rd party gateway to a Check Point security solution what object SHOULD be added? A(n):

- A. Interoperable Device
- B. Network Node
- C. Externally managed gateway
- D. Gateway

Answer: A

NEW QUESTION 203

- (Exam Topic 3)

Jennifer McHenry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.

To make this scenario work, the IT administrator must:

- 1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
- 2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
- 3) Create a new rule in the Firewall Rule Base to let Jennifer McHenry access network destinations. Select accept as the Action.
- 4) Install policy.

Ms McHenry tries to access the resource but is unable. What should she do?

- A. Have the security administrator select the Action field of the Firewall Rule "Redirect HTTP connections to an authentication (captive) portal".
- B. Have the security administrator reboot the firewall.
- C. Have the security administrator select Any for the Machines tab in the appropriate Access Role.
- D. Install the Identity Awareness agent on her iPad.

Answer: A

NEW QUESTION 208

- (Exam Topic 3)

A Cleanup rule:

- A. logs connections that would otherwise be dropped without logging by default.
- B. drops packets without logging connections that would otherwise be dropped and logged by default.
- C. logs connections that would otherwise be accepted without logging by default.
- D. drops packets without logging connections that would otherwise be accepted and logged by default.

Answer: A

NEW QUESTION 209

- (Exam Topic 3)

Which command can you use to enable or disable multi-queue per interface?

- A. cpmq set
- B. Cpmqueue set
- C. Cpmq config
- D. Set cpmq enable

Answer: A

NEW QUESTION 211

- (Exam Topic 3)

Which of the following is NOT a valid option when configuring access for Captive Portal?

- A. From the Internet
- B. Through internal interfaces
- C. Through all interfaces
- D. According to the Firewall Policy

Answer: A

NEW QUESTION 215

- (Exam Topic 3)

Which of the following actions do NOT take place in IKE Phase 1?

- A. Peers agree on encryption method.
- B. Diffie-Hellman key is combined with the key material to produce the symmetrical IPsec key.
- C. Peers agree on integrity method.
- D. Each side generates a session key from its private key and peer's public key.

Answer: B

NEW QUESTION 217

- (Exam Topic 3)

What is the difference between an event and a log?

- A. Events are generated at gateway according to Event Policy
- B. A log entry becomes an event when it matches any rule defined in Event Policy
- C. Events are collected with SmartWorkflow from Trouble Ticket systems
- D. Logs and Events are synonyms

Answer: B

NEW QUESTION 222

- (Exam Topic 3)

Match the following commands to their correct function. Each command has one function only listed.

- A. C1>F6; C2>F4; C3>F2; C4>F5
- B. C1>F2; C2>F1; C3>F6; C4>F4
- C. C1>F2; C2>F4; C3>F1; C4>F5
- D. C1>F4; C2>F6; C3>F3; C4>F5

Answer: A

NEW QUESTION 224

- (Exam Topic 3)

Review the rules. 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.

Answer: D

NEW QUESTION 225

- (Exam Topic 3)

A digital signature:

- A. Guarantees the authenticity and integrity of a message.
- B. Automatically exchanges shared keys.
- C. Decrypts data to its original form.
- D. Provides a secure key exchange mechanism over the Internet.

Answer: A

NEW QUESTION 226

- (Exam Topic 3)

The technical-support department has a requirement to access an intranet server. When configuring a User Authentication rule to achieve this, which of the following should you remember?

- A. You can only use the rule for Telnet, FTP, SMTP, and rlogin services.
- B. The Security Gateway first checks if there is any rule that does not require authentication for this type of connection before invoking the Authentication Security Server.
- C. Once a user is first authenticated, the user will not be prompted for authentication again until logging out.
- D. You can limit the authentication attempts in the User Properties' Authentication tab.

Answer: B

NEW QUESTION 231

- (Exam Topic 3)

On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

- A. 18210
- B. 18184
- C. 257
- D. 18191

Answer: B

NEW QUESTION 235

- (Exam Topic 3)

Which of the following authentication methods can be configured in the Identity Awareness setup wizard?

- A. Check Point Password
- B. TACACS
- C. LDAP
- D. Windows password

Answer: C

NEW QUESTION 239

- (Exam Topic 3)

What is the Manual Client Authentication TELNET port?

- A. 23
- B. 264
- C. 900
- D. 259

Answer: D

NEW QUESTION 242

- (Exam Topic 3)

Where does the security administrator activate Identity Awareness within SmartDashboard?

- A. Gateway Object > General Properties
- B. Security Management Server > Identity Awareness
- C. Policy > Global Properties > Identity Awareness
- D. LDAP Server Object > General Properties

Answer: A

NEW QUESTION 243

- (Exam Topic 3)

You are using SmartView Tracker to troubleshoot NAT entries. Which column do you check to view the NAT'd source port if you are using Source NAT?

- A. XlateDst
- B. XlateSPort
- C. XlateDPort
- D. XlateSrc

Answer: B

NEW QUESTION 244

- (Exam Topic 3)

Which of the following firewall modes DOES NOT allow for Identity Awareness to be deployed?

- A. Bridge
- B. Load Sharing
- C. High Availability
- D. Fail Open

Answer: A

NEW QUESTION 247

- (Exam Topic 3)

Katie has been asked to do a backup on the Blue Security Gateway. Which command would accomplish this in the Gaia CLI?

- A. Blue > add local backup
- B. Expert&Blue#add local backing
- C. Blue > set backup local
- D. Blue > add backup local

Answer: D

NEW QUESTION 249

- (Exam Topic 3)

While in SmartView Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion. He decides to block the traffic for 60 minutes, but cannot remember all the steps. What is the correct order of steps needed to set up the block?

- 1) Select Active Mode tab in SmartView Tracker.
- 2) Select Tools > Block Intruder.
- 3) Select Log Viewing tab in SmartView Tracker.
- 4) Set Blocking Timeout value to 60 minutes.
- 5) Highlight connection that should be blocked.

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

Answer: C

NEW QUESTION 252

- (Exam Topic 3)

Which one of the following is true about Threat Extraction?

- A. Always delivers a file to user
- B. Works on all MS Office, Executables, and PDF files
- C. Can take up to 3 minutes to complete
- D. Delivers file only if no threats found

Answer: B

NEW QUESTION 254

- (Exam Topic 3)

Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

- A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
- B. mgmt_cli add host name "Server_1" ip_address "10.15.123.10" --format json
- C. mgmt_cli add object-host "Server_1" ip_address "10.15.123.10" --format json
- D. mgmt_cli add object "Server_1" ip_address "10.15.123.10" --format json

Answer: A

NEW QUESTION 259

- (Exam Topic 3)

How do you configure an alert in SmartView Monitor?

- A. An alert cannot be configured in SmartView Monitor.
- B. By choosing the Gateway, and Configure Thresholds.
- C. By right-clicking on the Gateway, and selecting Properties.
- D. By right-clicking on the Gateway, and selecting System Information.

Answer: B

NEW QUESTION 260

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 261

- (Exam Topic 3)

Which component functions as the Internal Certificate Authority for R77?

- A. Security Gateway
- B. Management Server
- C. Policy Server
- D. SmartLSM

Answer: B

NEW QUESTION 262

- (Exam Topic 3)

All R77 Security Servers can perform authentication with the exception of one. Which of the Security Servers can NOT perform authentication?

- A. FTP
- B. SMTP
- C. HTTP
- D. RLOGIN

Answer: B

NEW QUESTION 265

- (Exam Topic 3)

What are types of Check Point APIs available currently as part of R80.10 code?

- A. Security Gateway API, Management API, Threat Prevention API and Identity Awareness Web Services API
- B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
- C. OSE API, OPSEC SDK API, Threat Prevention API and Policy Editor API
- D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

NEW QUESTION 267

- (Exam Topic 3)

You have configured SNX on the Security Gateway. The client connects to the Security Gateway and the user enters the authentication credentials. What must happen after authentication that allows the client to connect to the Security Gateway's VPN domain?

- A. SNX modifies the routing table to forward VPN traffic to the Security Gateway.
- B. An office mode address must be obtained by the client.
- C. The SNX client application must be installed on the client.
- D. Active-X must be allowed on the client.

Answer: A

NEW QUESTION 269

- (Exam Topic 3)

You have just installed your Gateway and want to analyze the packet size distribution of your traffic with SmartView Monitor.

Unfortunately, you get the message:

"There are no machines that contain Firewall Blade and SmartView Monitor".

What should you do to analyze the packet size distribution of your traffic? Give the BEST answer.

- A. Purchase the SmartView Monitor license for your Security Management Server.
- B. Enable Monitoring on your Security Management Server.
- C. Purchase the SmartView Monitor license for your Security Gateway.
- D. Enable Monitoring on your Security Gateway.

Answer: D

NEW QUESTION 270

- (Exam Topic 4)

What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?

- A. S
- B. W
- C. C
- D. Space bar

Answer: B

NEW QUESTION 271

- (Exam Topic 4)

How are the backups stored in Chock Point appliances?

- A. Saved as * .tar under /var/log/Cpbackup/backups
- B. Saved as * .tgz under /var/cppbackup
- C. Saved as * .tar under /var/cppbackup
- D. Saved as * .tgz under /var/log/CPbackup/backups

Answer: D

NEW QUESTION 272

- (Exam Topic 4)

The CDT utility supports which of the following?

- A. Major version upgrades to R77.30
- B. Only Jumbo HFA's and hotfixes
- C. Only major version upgrades to R80.10
- D. All upgrades

Answer: D

NEW QUESTION 276

- (Exam Topic 4)

What is the BEST method to deploy identity Awareness for roaming users?

- A. Use Office Mode
- B. Use identity agents
- C. Share user identities between gateways
- D. Use captive portal

Answer: A

NEW QUESTION 279

- (Exam Topic 4)

Which one of the following is TRUE?

- A. Ordered policy is a sub-policy within another policy
- B. One policy can be either inline or ordered, but not both
- C. Inline layer can be defined as a rule action
- D. Pre-R80 Gateways do not support ordered layers

Answer: C

NEW QUESTION 282

- (Exam Topic 4)

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

- A. fwd
- B. fwm
- C. cpd
- D. cpwd

Answer: B

NEW QUESTION 286

- (Exam Topic 4)

Which identity Source(s) should be selected in Identity Awareness for when there is a requirement for a higher level of security for sensitive servers?

- A. ADQuery
- B. Terminal Servers Endpoint Identity Agent
- C. Endpoint Identity Agent and Browser-Based Authentication
- D. RADIUS and Account Logon

Answer: D

NEW QUESTION 287

- (Exam Topic 4)

What does it mean if Deyra sees the gateway status

Choose the BEST answer.

- A. SmartCenter Server cannot reach this Security Gateway
- B. There is a blade reporting a problem
- C. VPN software blade is reporting a malfunction
- D. Security Gateway s MGNT NIC card is disconnected

Answer: A

NEW QUESTION 292

- (Exam Topic 4)

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R80 configuration, clean install R80.10 and import the configuration
- B. CPUSE online upgrade
- C. CPUSE offline upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 296

- (Exam Topic 4)

Which of the following is NOT a component of Check Point Capsule?

- A. Capsule Docs
- B. Capsule Cloud
- C. Capsule Enterprise
- D. Capsule Workspace

Answer: C

NEW QUESTION 301

- (Exam Topic 4)

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

- A. Next Generation Threat Prevention
- B. Next Generation Threat Emulation
- C. Next Generation Threat Extraction
- D. Next Generation Firewall

Answer: B

NEW QUESTION 304

- (Exam Topic 4)

When logging in for the first time to a Security management Server through SmartConsole, a fingerprint is saved to the:

- A. Security Management Server's /home/.fgpt file and is available for future SmartConsole authentications.
- B. Windows registry is available for future Security Management Server authentications.
- C. there is no memory used for saving a fingerprint anyway.
- D. SmartConsole cache is available for future Security Management Server authentications.

Answer: D

NEW QUESTION 307

- (Exam Topic 4)

Fill in the blank: Authentication rules are defined for ____ .

- A. User groups
- B. Users using UserCheck
- C. Individual users
- D. All users in the database

Answer: A

NEW QUESTION 312

- (Exam Topic 4)

Administrator Dave logs into R80 Management Server to review and makes some rule changes. He notices that there is a padlock sign next to the DNS rule in the Rule Base.

What is the possible Explanation: for this?

- A. DNS Rule is using one of the new feature of R80 where an administrator can mark a rule with the padlock icon to let other administrators know it is important.
- B. Another administrator is logged into the Management and currently editing the DNS Rule.
- C. DNS Rule is a placeholder rule for a rule that existed in the past but was deleted.
- D. This is normal behavior in R80 when there are duplicate rules in the Rule Base.

Answer: B

NEW QUESTION 317

- (Exam Topic 4)

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- A. SND is a feature to accelerate multiple SSL VPN connections
- B. SND is an alternative to IPSec Main Mode, using only 3 packets
- C. SND is used to distribute packets among Firewall instances
- D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

NEW QUESTION 318

- (Exam Topic 4)

Which SmartConsole tab shows logs and detects security threats, providing a centralized display of potential attack patterns from all network devices?

- A. Gateway and Servers
- B. Logs and Monitor
- C. Manage Setting
- D. Security Policies

Answer: B

NEW QUESTION 321

- (Exam Topic 4)

Using ClusterXL, what statement is true about the Sticky Decision Function?

- A. Can only be changed for Load Sharing implementations
- B. All connections are processed and synchronized by the pivot
- C. Is configured using cpconfig
- D. Is only relevant when using SecureXL

Answer: A

NEW QUESTION 322

- (Exam Topic 4)

What is the purpose of the Clean-up Rule?

- A. To log all traffic that is not explicitly allowed or denied in the Rule Base.
- B. To clean up policies found inconsistent with the compliance blade reports.
- C. To remove all rules that could have a conflict with other rules in the database.
- D. To eliminate duplicate log entries in the Security Gateway

Answer: A

NEW QUESTION 327

- (Exam Topic 4)

What is the best sync method in the ClusterXL deployment?

- A. Use 1 cluster + 1st sync
- B. Use 1 dedicated sync interface
- C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
- D. Use 2 clusters + 1st sync + 2nd sync

Answer: B

NEW QUESTION 331

- (Exam Topic 4)

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network
- B. Network and Threat Prevention
- C. Application Control and URL Filtering
- D. Network and Application Control

Answer: C

NEW QUESTION 332

- (Exam Topic 4)

Fill in the blank: To create policy for traffic to or from a particular location, use the_____ .

- A. DLP shared policy
- B. Geo policy shared policy
- C. Mobile Access software blade
- D. HTTPS inspection

Answer: B

Explanation:

Shared Policies

The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages.

Shared policies are installed with the Access Control Policy. Software Blade

Description Mobile Access

Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.

DLP Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.

Geo Policy

Create a policy for traffic to or from specific geographical or political locations. References:

NEW QUESTION 334

- (Exam Topic 4)

Which of the following is an authentication method used for Identity Awareness?

- A. SSL
- B. Captive Portal
- C. PKI
- D. RSA

Answer: B

NEW QUESTION 337

- (Exam Topic 4)

What SmartEvent component creates events?

- A. Consolidation Policy
- B. Correlation Unit
- C. SmartEvent Policy
- D. SmartEvent GUI

Answer: B

NEW QUESTION 339

- (Exam Topic 4)

Which firewall daemon is responsible for the FW CLI commands?

- A. fwd
- B. fwm
- C. cpm
- D. cpd

Answer: A

NEW QUESTION 341

- (Exam Topic 4)

Fill in the blanks. There are _____ types of software containers _____

- A. Three; security management
- B. Security Gateway and endpoint security.
- C. Three; Security Gateway, endpoint Security, and gateway management.
- D. Two; security management and endpoint security
- E. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 345

- (Exam Topic 4)

When a Security Gateways sends its logs to an IP address other than its own, which deployment option is installed?

- A. Distributed
- B. Standalone
- C. Bridge

Answer: A

NEW QUESTION 350

- (Exam Topic 4)

In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

- A. Accounting
- B. Suppression
- C. Accounting/Suppression
- D. Accounting/Extended

Answer: C

NEW QUESTION 353

- (Exam Topic 4)

Access roles allow the firewall administrator to configure Network access according to:

- A. a combination of computer or computer groups and network
- B. users and user groups
- C. all of above
- D. remote access clients

Answer: C

NEW QUESTION 354

- (Exam Topic 4)

When installing a dedicated R80 SmartEvent server, what is the recommended size of the root partition?

- A. Any size
- B. Less than 20GB
- C. More than 10GB and less than 20 GB
- D. At least 20GB

Answer: D

NEW QUESTION 355

- (Exam Topic 4)

When an encrypted packet is decrypted, where does this happen?

- A. Security policy
- B. Inbound chain
- C. Outbound chain
- D. Decryption is not supported

Answer: A

NEW QUESTION 356

- (Exam Topic 4)

Under which file is the proxy arp configuration stored?

- A. \$FWDIR/state/proxy_arp.conf on the management server
- B. \$FWDIR/conf/local.arp on the management server
- C. \$FWDIR/state/_tmp/proxy.arp on the security gateway
- D. \$FWDIR/conf/local.arp on the gateway

Answer: D

NEW QUESTION 358

- (Exam Topic 4)

When using Monitored circuit VRRP, what is a priority delta?

- A. When an interface fails the priority changes to the priority delta
- B. When an interface fails the delta claims the priority
- C. When an interface fails the priority delta is subtracted from the priority
- D. When an interface fails the priority delta decides if the other interfaces takes over

Answer: C

NEW QUESTION 359

- (Exam Topic 4)

What is the BEST command to view configuration details of all interfaces in Gaia CLISH?

- A. ifconfig -a
- B. show interfaces
- C. show interfaces detail
- D. show configuration interface

Answer: D

NEW QUESTION 361

- (Exam Topic 4)

You have discovered activity in your network. What is the BEST immediate action to take?

- A. Create a policy rule to block the traffic.
- B. Create a suspicious action rule to block that traffic.
- C. Wait until traffic has been identified before making any changes.
- D. Contact ISP to block the traffic.

Answer: B

NEW QUESTION 363

- (Exam Topic 4)

Which of the following methods can be used to update the trusted log server regarding the policy and configuration changes performed on the Security Management Server?

- A. Save Policy
- B. install Database
- C. Save Session
- D. install Policy

Answer: D

NEW QUESTION 368

- (Exam Topic 4)

Which of the following is NOT a tracking option?

- A. Partial log
- B. Log
- C. Network log
- D. Full log

Answer: A

NEW QUESTION 373

- (Exam Topic 4)

Fill in the blanks. In _____ NAT, the _____ is translated.

- A. Hide; source
- B. Static; source
- C. Simple; source
- D. Hide; destination

Answer:

B

NEW QUESTION 374

- (Exam Topic 4)

Which of the following is NOT a method used by Identity Awareness for acquiring identity?

- A. RADIUS
- B. Active Directory Query
- C. Remote Access
- D. Certificates

Answer: D

NEW QUESTION 376

- (Exam Topic 4)

Choose what BEST describes the reason why querying logs now is very fast.

- A. New Smart-1 appliances double the physical memory install
- B. Indexing Engine indexes logs for faster search results
- C. SmartConsole now queries results directly from the Security Gateway
- D. The amount of logs been store is less than the usual in older versions

Answer: B

NEW QUESTION 378

- (Exam Topic 4)

True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

- A. False, this feature has to be enabled in the Global Properties.
- B. True, every administrator works in a session that is independent of the other administrators.
- C. True, every administrator works on a different database that is independent of the other administrators.
- D. False, only one administrator can login with write permission.

Answer: B

Explanation:

More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

NEW QUESTION 381

- (Exam Topic 4)

Which SmartConsole tab is used to monitor network and security performance?

- A. Manage Seeting
- B. Security Policies
- C. Gateway and Servers
- D. Logs and Monitor

Answer: C

NEW QUESTION 386

- (Exam Topic 4)

Phase 1 of the two-phase negotiation process conducted by IKE operates in a _____ mode.

- A. Main
- B. Authentication
- C. Quick
- D. High Alert

Answer: A

NEW QUESTION 389

- (Exam Topic 4)

Which of the following is the most secure means of authentication?

- A. Password
- B. Certificate
- C. Token
- D. Pre-shared secret

Answer: B

NEW QUESTION 394

- (Exam Topic 4)

Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security

Gateway.

- A. Format; corporate
- B. Local; formal
- C. Local; central
- D. Central; local

Answer: D

NEW QUESTION 397

- (Exam Topic 4)

Which path below is available only when CoreXL is enabled?

- A. Slow path
- B. Firewall path
- C. Medium path
- D. Accelerated path

Answer: C

NEW QUESTION 399

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

156-215.80 Practice Exam Features:

- * 156-215.80 Questions and Answers Updated Frequently
- * 156-215.80 Practice Questions Verified by Expert Senior Certified Staff
- * 156-215.80 Most Realistic Questions that Guarantee you a Pass on Your First Try
- * 156-215.80 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-215.80 Practice Test Here](#)