

156-215.80 Dumps

Check Point Certified Security Administrator

<https://www.certleader.com/156-215.80-dumps.html>



NEW QUESTION 1

Which of the following is NOT a component of a Distinguished Name?

- A. Organization Unit
- B. Country
- C. Common name
- D. User container

Answer: D

Explanation: Distinguished Name Components

CN=common name, OU=organizational unit, O=organization, L=locality, ST=state or province, C=country name

NEW QUESTION 2

Which utility allows you to configure the DHCP service on GAIA from the command line?

- A. ifconfig
- B. dhcp_cfg
- C. sysconfig
- D. cpconfig

Answer: C

Explanation: Sysconfig Configuration Options

	Menu Item	Purpose
7	DHCP Server Configuration	Configure SecurePlatform DHCP Server.
8	DHCP Relay Configuration	Setup DHCP Relay.

NEW QUESTION 3

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 4

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the right protections in place. Check Point has been selected for the security vendor. Which Check Point products protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

- A. IPS and Application Control
- B. IPS, anti-virus and anti-bot
- C. IPS, anti-virus and e-mail security
- D. SandBlast

Answer: D

Explanation: SandBlast Zero-Day Protection

Hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. Zero-day exploit protection from Check Point provides a deeper level of inspection so you can prevent more malware and zero-day attacks, while ensuring quick delivery of safe content to your users.

NEW QUESTION 5

You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R80 gateways.

Answer: A

Explanation: The most likely reason for the logs data to stop is the low disk space on the logging device, which can be the Management Server or the Gateway Server.

NEW QUESTION 6

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

- A. SmartView Monitor
- B. SmartEvent
- C. SmartUpdate
- D. SmartDashboard

Answer: B

Explanation: SmartEvent correlates logs from all Check Point enforcement points, including end-points, to identify suspicious activity from the clutter. Rapid data analysis and custom event logs immediately alert administrators to anomalous behavior such as someone attempting to use the same credential in multiple geographies simultaneously.

NEW QUESTION 7

What are the three essential components of the Check Point Security Management Architecture?

- A. SmartConsole, Security Management Server, Security Gateway
- B. SmartConsole, SmartUpdate, Security Gateway
- C. Security Management Server, Security Gateway, Command Line Interface
- D. WebUI, SmartConsole, Security Gateway

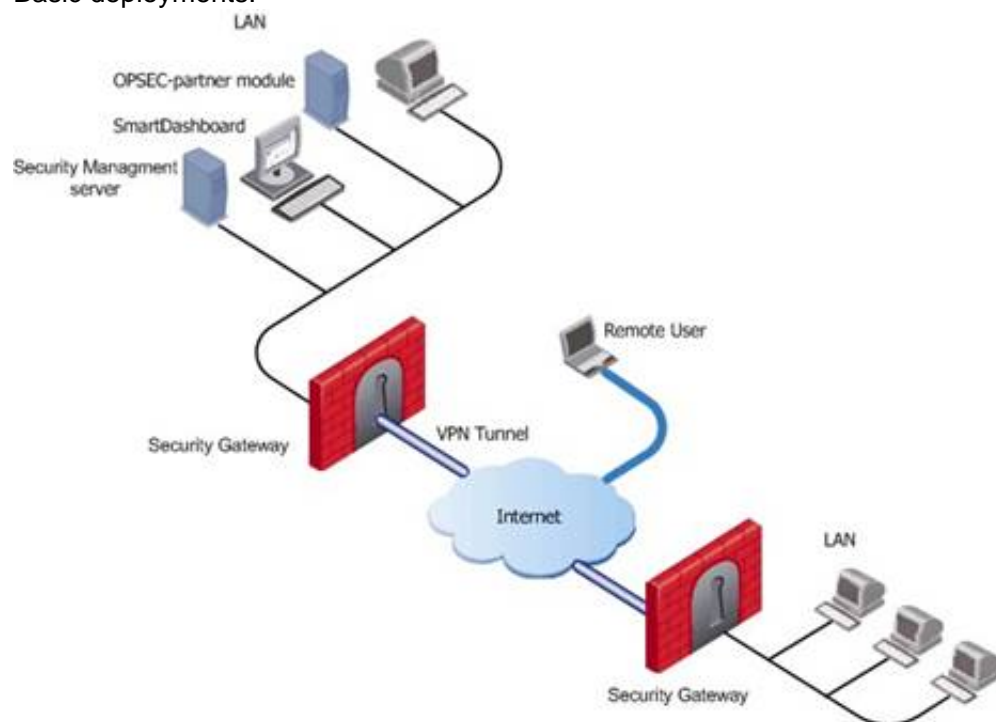
Answer: A

Explanation: Standalone deployment - Security Gateway and the Security Management server are installed on the same machine.

Distributed deployment - Security Gateway and the Security Management server are installed on different machines.

Deployments

Basic deployments:



Assume an environment with gateways on different sites. Each Security Gateway connects to the Internet on one side, and to a LAN on the other.

You can create a Virtual Private Network (VPN) between the two Security Gateways, to secure all communication between them.

The Security Management server is installed in the LAN, and is protected by a Security Gateway. The Security Management server manages the Security Gateways and lets remote users connect securely to the corporate network. SmartDashboard can be installed on the Security Management server or another computer.

There can be other OPSEC-partner modules (for example, an Anti-Virus Server) to complete the network security with the Security Management server and its Security Gateways.

NEW QUESTION 8

Which of the following statements is TRUE about R80 management plug-ins?

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

Answer: C

NEW QUESTION 9

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 10

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SmartConsole
- C. SecureClient
- D. SmartEvent

Answer: D

Explanation: There are different deployment scenarios for Check Point software products.

Standalone Deployment - The Security Management Server and the Security Gateway are installed on the same computer or appliance.

NEW QUESTION 10

The Gaia operating system supports which routing protocols?

- A. BGP, OSPF, RIP
- B. BGP, OSPF, EIGRP, PIM, IGMP
- C. BGP, OSPF, RIP, PIM, IGMP
- D. BGP, OSPF, RIP, EIGRP

Answer: A

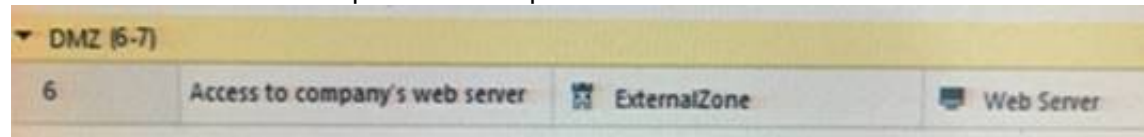
Explanation: The Advanced Routing Suite

The Advanced Routing Suite CLI is available as part of the Advanced Networking Software Blade.

For organizations looking to implement scalable, fault-tolerant, secure networks, the Advanced Networking blade enables them to run industry-standard dynamic routing protocols including BGP, OSPF, RIPv1, and RIPv2 on security gateways. OSPF, RIPv1, and RIPv2 enable dynamic routing over a single autonomous system—like a single department, company, or service provider—to avoid network failures. BGP provides dynamic routing support across more complex networks involving multiple autonomous systems—such as when a company uses two service providers or divides a network into multiple areas with different administrators responsible for the performance of each.

NEW QUESTION 12

What does ExternalZone represent in the presented rule?



- A. The Internet.
- B. Interfaces that administrator has defined to be part of External Security Zone.
- C. External interfaces on all security gateways.
- D. External interfaces of specific gateways.

Answer: B

Explanation: Configuring Interfaces

Configure the Security Gateway 80 interfaces in the Interfaces tab in the Security Gateway window. To configure the interfaces:

From the Devices window, double-click the Security Gateway 80.

The Security Gateway

window opens.

Select the Interfaces tab.

Select Use the following settings. The interface settings open.

Select the interface and click Edit.

The Edit window opens.

From the IP Assignment section, configure the IP address of the interface:

Select Static IP.

Enter the IP address and subnet mask for the interface.

In Security Zone, select Wireless, DMS, External, or Internal. Security zone is a type of zone, created by a bridge to easily create segments, while maintaining IP addresses and router configurations. Security zones let you choose if to enable or not the firewall between segments.

References:

NEW QUESTION 17

Which default user has full read/write access?

- A. Monitor
- B. Altuser
- C. Administrator
- D. Superuser

Answer: C

NEW QUESTION 19

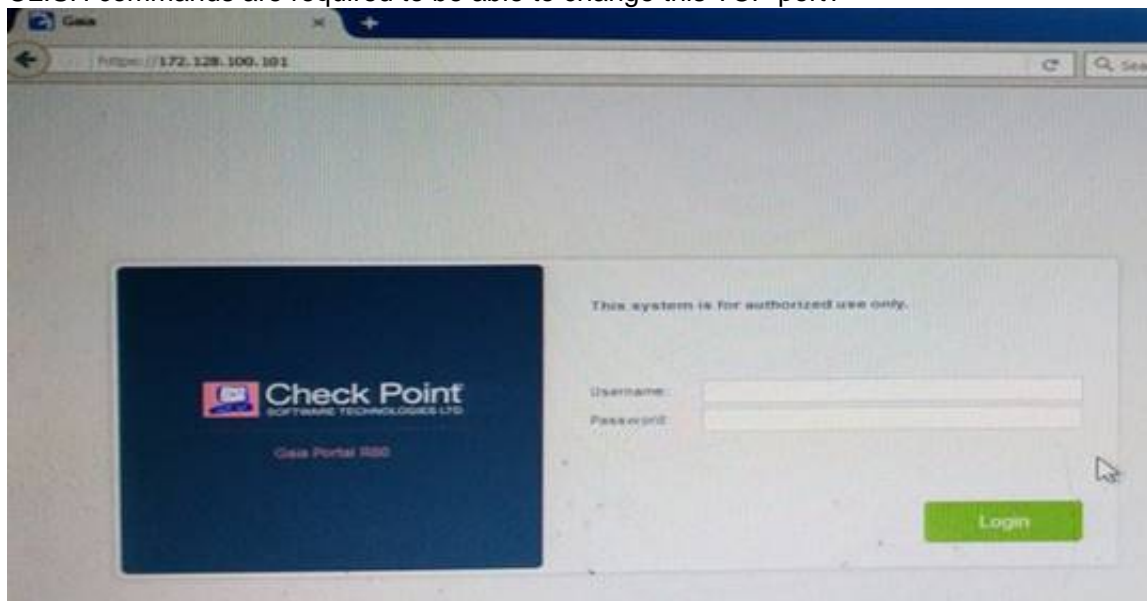
Which of the following is TRUE regarding Gaia command line?

- 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 24

Kofi, the administrator of the ABC Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



- A. set web ssl-port <new port number>
- B. set Gaia-portal <new port number>
- C. set Gaia-portal https-port <new port number>
- D. set web https-port <new port number>

Answer: A

Explanation: In Clish

Connect to command line on Security Gateway / each

Log in to Clish.

Set the desired port (e.g., port 4434):

Cluster member.

HostName> set web ssl-port <Port_Number>

Save the changes:

HostName> save config

Verify that the configuration was saved:

[Expert@HostName]# grep 'httpd:ssl_port' /config/db/initial References:

NEW QUESTION 26

Fill in the blank: The R80 utility fw monitor is used to troubleshoot _____

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues
- D. Phase two key negotiation

Answer: C

Explanation: Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark

NEW QUESTION 28

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 31

Which of the following Automatically Generated Rules NAT rules have the lowest implementation priority?

- A. Machine Hide NAT
- B. Address Range Hide NAT
- C. Network Hide NAT
- D. Machine Static NAT

Answer: BC

Explanation: SmartDashboard organizes the automatic NAT rules in this order:

Static NAT rules for Firewall, or node (computer or server) objects

Hide NAT rules for Firewall, or node objects

Static NAT rules for network or address range objects

Hide NAT rules for network or address range objects

References:

NEW QUESTION 33

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 36

What is the default shell for the command line interface?

- A. Expert
- B. Clish
- C. Admin
- D. Normal

Answer: B

Explanation: The default shell of the CLI is called clish References:

NEW QUESTION 41

Which of the following is NOT an authentication scheme used for accounts created through SmartConsole?

- A. Security questions
- B. Check Point password
- C. SecurID
- D. RADIUS

Answer: A

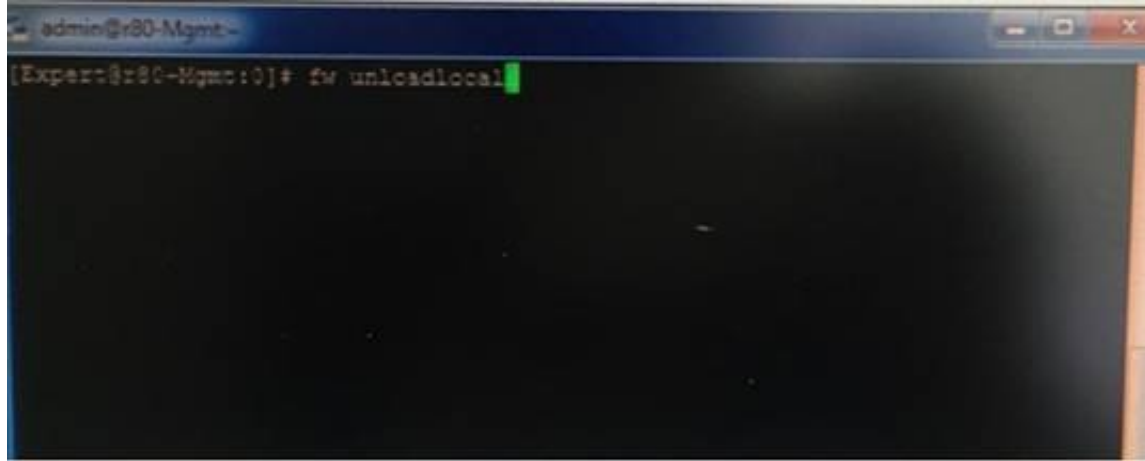
Explanation: Authentication Schemes :- Check Point Password

- Operating System Password
- RADIUS
- SecurID

- TACAS
- Undefined If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, access is always denied.

NEW QUESTION 43

What will be the effect of running the following command on the Security Management Server?



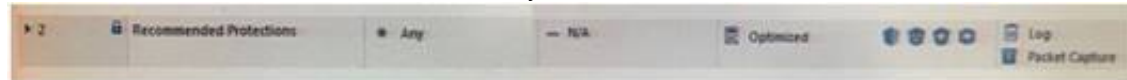
- A. Remove the installed Security Policy.
- B. Remove the local ACL lists.
- C. No effect.
- D. Reset SIC on all gateways.

Answer: A

Explanation: This command uninstall actual security policy (already installed) References:

NEW QUESTION 47

View the rule below. What does the lock-symbol in the left column mean? Select the BEST answer.



- A. The current administrator has read-only permissions to Threat Prevention Policy.
- B. Another user has locked the rule for editing.
- C. Configuration lock is present
- D. Click the lock symbol to gain read-write access.
- E. The current administrator is logged in as read-only because someone else is editing the policy.

Answer: B

Explanation: Administrator Collaboration

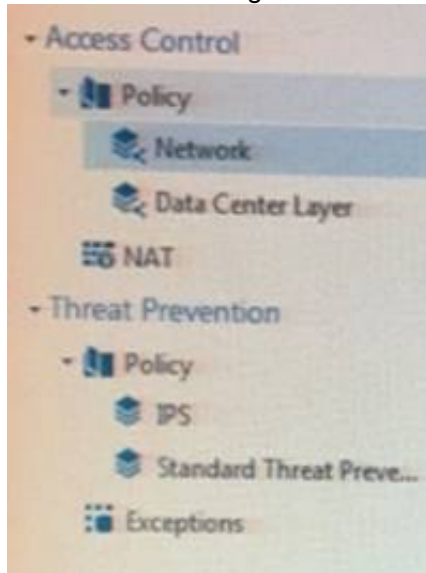
More than one administrator can connect to the Security Management Server at the same time. Every administrator has their own username, and works in a session that is independent of the other administrators.

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 51

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 54

Joey wants to configure NTP on R80 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

- A. `https://<Device_IP_Address>`
- B. `https://<Device_IP_Address>:443`
- C. `https://<Device_IP_Address>:10000`
- D. `https://<Device_IP_Address>:4434`

Answer: A

Explanation: Access to Web UI Gaia administration interface, initiate a connection from a browser to the default administration IP address: Logging in to the WebUI

Logging in

To log in to the WebUI:

Enter this URL in your browser: `https://<Gaia IP address>`

Enter your user name and password. References:

NEW QUESTION 58

Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

- A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
- B. One machine
- C. Two machines
- D. Three machines

Answer: C

Explanation: One for Security Management Server and the other one for the Security Gateway.

NEW QUESTION 62

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 64

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.

Description	Use the <code>lock database override</code> and <code>unlock database</code> commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	<ul style="list-style-type: none">o <code>lock database override</code>o <code>unlock database</code>

NEW QUESTION 68

Choose what BEST describes the Policy Layer Traffic Inspection.

- A. If a packet does not match any of the inline layers, the matching continues to the next Layer.
- B. If a packet matches an inline layer, it will continue matching the next layer.
- C. If a packet does not match any of the inline layers, the packet will be matched against the Implicit Clean-up Rule.
- D. If a packet does not match a Network Policy Layer, the matching continues to its inline layer.

Answer: B

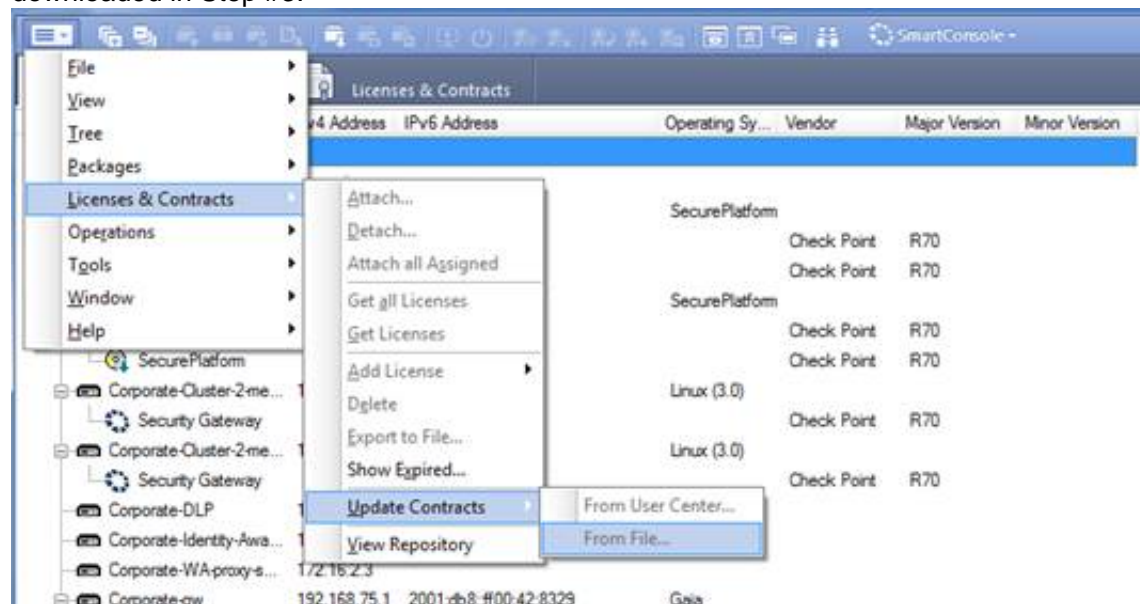
NEW QUESTION 70

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 74

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 77

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 81

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

- A. To satellites through center only
- B. To center only
- C. To center and to other satellites through center
- D. To center, or through the center to other satellites, to internet and other VPN targets

Answer: D

Explanation: On the VPN Routing page, enable the VPN routing for satellites section, by selecting one of these options:

To center and to other Satellites through center; this allows connectivity between Gateways; for example, if the spoke Gateways are DAIP Gateways, and the hub is a Gateway with a static IP address

To center, or through the center to other satellites, to Internet and other VPN targets; this allows connectivity between the Gateways, as well as the ability to inspect all communication passing through the hub to the Internet.

NEW QUESTION 82

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 87

The following graphic shows:

[illegible]

- A. View from SmartLog for logs initiated from source address 10.1.1.202
B. View from SmartView Tracker for logs of destination address 10.1.1.202
C. View from SmartView Tracker for logs initiated from source address 10.1.1.202
D. View from SmartView Monitor for logs initiated from source address 10.1.1.202

Answer: C

NEW QUESTION 90

Which of the following is NOT an integral part of VPN communication within a network?

- A. VPN key
- B. VPN community
- C. VPN trust entities
- D. VPN domain

Answer: A

Explanation: VPN key (to not be confused with pre-shared key that is used for authentication).

VPN trust entities, such as a Check Point Internal Certificate Authority (ICA). The ICA is part of the Check Point suite used for creating SIC trusted connection between Security Gateways, authenticating administrators and third party servers. The ICA provides certificates for internal Security Gateways and remote access clients which negotiate the VPN link.

VPN Domain - A group of computers and networks connected to a VPN tunnel by one VPN gateway that handles encryption and protects the VPN Domain members.

VPN Community - A named collection of VPN domains, each protected by a VPN gateway. References:

http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

NEW QUESTION 94

Fill in the blank: Gaia can be configured using the _____ or _____.

- A. Gaia; command line interface
B. WebUI; Gaia Interface
C. Command line interface; WebUI
D. Gaia Interface; GaiaUI

Answer: C

Explanation: Configuring Gaia for the First Time In This Section:

Running the First Time Configuration Wizard in WebUI Running the First Time Configuration Wizard in CLI

After you install Gaia for the first time, use the First Time Configuration Wizard to configure the system and the Check Point products on it.

NEW QUESTION 99

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 101

What is the order of NAT priorities?

- A. Static NAT, IP pool NAT, hide NAT
- B. IP pool NAT, static NAT, hide NAT
- C. Static NAT, automatic NAT, hide NAT
- D. Static NAT, hide NAT, IP pool NAT

Answer: A

Explanation: The order of NAT priorities is:

Static NAT
IP Pool NAT
Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

NEW QUESTION 102

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CApp

Answer: B

Explanation: AppWiki Application Classification Library

AppWiki enables application scanning and detection of more than 5,000 distinct applications and over 300,000 Web 2.0 widgets including instant messaging, social networking, video streaming, VoIP, games and more.

NEW QUESTION 105

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret is shared and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

Answer: C

NEW QUESTION 107

Which of the following is NOT a license activation method?

- A. SmartConsole Wizard
- B. Online Activation
- C. License Activation Wizard
- D. Offline Activation

Answer: A

NEW QUESTION 108

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 113

In R80, Unified Policy is a combination of

- A. Access control policy, QoS Policy, Desktop Security Policy and endpoint policy.
- B. Access control policy, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- C. Firewall policy, address Translation and application and URL filtering, QoS Policy, Desktop Security Policy and Threat Prevention Policy.
- D. Access control policy, QoS Policy, Desktop Security Policy and VPN policy.

Answer: D

Explanation: D is the best answer given the choices. Unified Policy

In R80 the Access Control policy unifies the policies of these pre-R80 Software Blades:

Firewall and VPN
Application Control and URL Filtering
Identity Awareness
Data Awareness
Mobile Access
Security Zones

NEW QUESTION 116

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 gatewa 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 119

If there are two administrators logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available to other administrators? Choose the BEST answer.

- A. Publish or discard the session.
- B. Revert the session.
- C. Save and install the Policy.
- D. Delete older versions of database.

Answer: A

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

To make your changes available to other administrators, and to save the database before installing a policy, you must publish the session. When you publish a session, a new database version is created.

When you select Install Policy, you are prompted to publish all unpublished changes. You cannot install a policy if the included changes are not published.

NEW QUESTION 122

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 123

Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

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

Answer: D

NEW QUESTION 124

Fill in the blank: The tool ____ generates a R80 Security Gateway configuration report.

- A. infoCP
- B. infoview
- C. cpinfo
- D. fw cpinfo

Answer: C

Explanation: CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPinfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPinfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

When contacting Check Point Support, collect the cpinfo files from the Security Management server and Security Gateways involved in your case.

NEW QUESTION 127

When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

- A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
- B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
- C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
- D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Answer: C

NEW QUESTION 131

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 132

Which policy type has its own Exceptions section?

- A. Thread Prevention
- B. Access Control
- C. Threat Emulation
- D. Desktop Security

Answer: A

Explanation: The Exceptions Groups pane lets you define exception groups. When necessary, you can create exception groups to use in the Rule Base. An exception group contains one or more defined exceptions. This option facilitates ease-of-use so you do not have to manually define exceptions in multiple rules for commonly required exceptions. You can choose to which rules you want to add exception groups. This means they can be added to some rules and not to others, depending on necessity.

NEW QUESTION 134

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

Method	To Stop ClusterXL	To Start ClusterXL
Run: <ul style="list-style-type: none"> o <code>cphaprob -d faildevice -t 0 -s ok register</code> o <code>cphaprob -d faildevice -s problem report</code> and: <ul style="list-style-type: none"> o <code>cphaprob -d faildevice -s ok report</code> o <code>cphaprob -d faildevice unregister</code> 	Effect: <ul style="list-style-type: none"> o Disables ClusterXL o Does not disable synchronization 	Effect: <ul style="list-style-type: none"> o Enables ClusterXL o Does not initiate full synchronization
Recommended method: Run: <ul style="list-style-type: none"> o <code>clusterXL_admin down</code> o <code>clusterXL_admin up</code> 	<ul style="list-style-type: none"> o Disables ClusterXL o Does not disable synchronization 	<ul style="list-style-type: none"> o Enables ClusterXL o Does not initiate full synchronization
In SmartView Monitor: <ol style="list-style-type: none"> 1. Click the Cluster object. 2. Select one of the member gateway branches. 3. Right click the cluster member. 4. Select Down. 	<ul style="list-style-type: none"> o Disables ClusterXL o Disables synchronization 	<ul style="list-style-type: none"> o Enables ClusterXL o Does not initiate full synchronization

NEW QUESTION 136

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

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

NEW QUESTION 138

Harriet wants to protect sensitive information from intentional loss when users browse to a specific URL: <https://personal.mymail.com>, which blade will she enable to achieve her goal?

- A. DLP
- B. SSL Inspection
- C. Application Control
- D. URL Filtering

Answer: A

Explanation: Check Point revolutionizes DLP by combining technology and processes to move businesses from passive detection to active Data Loss Prevention. Innovative MultiSpect™ data classification combines user, content and process information to make accurate decisions, while UserCheck™ technology empowers users to remediate incidents in real time. Check Point's self-educating network-based DLP solution frees IT/security personnel from incident handling and educates users on proper data handling policies—protecting sensitive corporate information from both intentional and unintentional loss.

NEW QUESTION 142

Which feature is NOT provided by all Check Point Mobile Access solutions?

- A. Support for IPv6
- B. Granular access control
- C. Strong user authentication
- D. Secure connectivity

Answer: A

Explanation: Types of Solutions

Enterprise-grade, secure connectivity to corporate resources.
Strong user authentication.

Granular access control. References:

NEW QUESTION 144

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

APP	PID	STAT	#START	START_TIME	MON	COMMAND
CPVIEW	1078	E	1	[16:26:34] 5/5/2016	N	cpviewd
CPD	0	T	1	[17:13:37] 6/5/2016	N	cpd
FWD	21781	E	1	[17:13:31] 6/5/2016	N	fwd -s
CPM	0	T	1	[16:32:23] 6/5/2016	N	/opt/CPsuite-830/fwL/scripts/cpm.sh -s
FWM	0	T	1	[17:13:45] 6/5/2016	N	fwm
SQL	7873	E	1	[16:32:32] 5/5/2016	N	LogCore
SMARTVIEW	7884	E	1	[16:32:32] 5/5/2016	N	SmartView
INDEXER	7894	E	1	[16:32:33] 5/5/2016	N	/opt/CPsuite-830/log_indexer/log_indexer
SMARTLOG_SERVER	7877	E	1	[16:32:33] 5/5/2016	N	/opt/CPsmartlog-830/smartlog_server
SVR	8045	E	1	[16:32:34] 5/5/2016	N	SVRServer
DASERVICE	8034	E	1	[16:32:34] 5/5/2016	N	DAService_script
CPSM	0	T	0	[17:17:02] 6/5/2016	N	cpstat_monitor

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 147

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 152

Examine the following Rule Base.

Rule	Name	Source	Destination	Action	Services & Applications	Status
1	Do not log	Any	Any	Log	HTTP	Enabled
2	Allow Http	Any	Any	Accept	Web	Disabled
3	Deny Http	Any	Any	Drop	Web	Disabled
4	Web Server	Any	Any	Accept	Web	Disabled
5	Web Server	Any	Any	Accept	Web	Disabled
6	Web Server	Any	Any	Accept	Web	Disabled
7	Web Server	Any	Any	Accept	Web	Disabled
8	Web Server	Any	Any	Accept	Web	Disabled

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)

	Description
	Discard changes made during the session
	Enter session details and see the number of changes made in the session
	Commit policy changes to the database and make them visible to other administrators Note - The changes are saved on the gateways and enforced after the next policy install

NEW QUESTION 153

Which Threat Prevention Software Blade provides comprehensive against malicious and unwanted network traffic, focusing on application and server vulnerabilities?

- A. Anti-Virus
- B. IPS
- C. Anti-Spam
- D. Anti-bot

Answer: B

Explanation: The IPS Software Blade provides a complete Intrusion Prevention System security solution, providing comprehensive network protection against malicious and unwanted network traffic, including:

Malware attacks
Dos and DDoS attacks
Application and server vulnerabilities
Insider threats
Unwanted application traffic, including IM and P2P

NEW QUESTION 154

What are the two types of address translation rules?

- A. Translated packet and untranslated packet
- B. Untranslated packet and manipulated packet
- C. Manipulated packet and original packet
- D. Original packet and translated packet

Answer: D

Explanation: NAT Rule Base

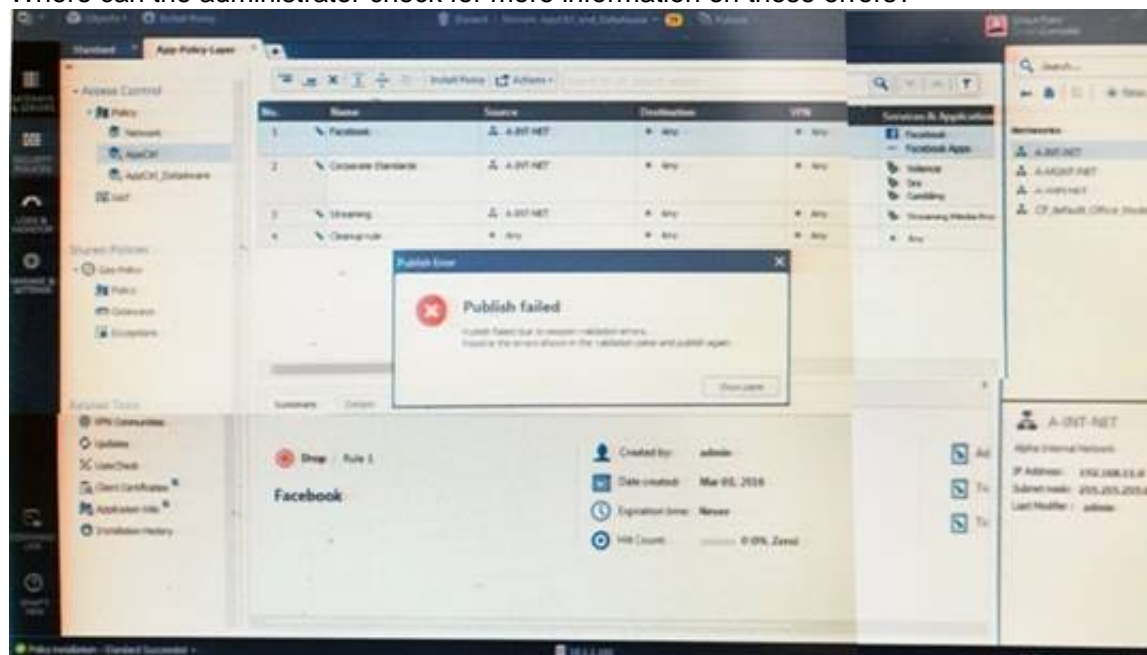
The NAT Rule Base has two sections that specify how the IP addresses are translated:

Original Packet
Translated Packet References:

NEW QUESTION 157

Administrator Kofi has just made some changes on his Management Server and then clicks on the Publish button in SmartConsole but then gets the error message shown in the screenshot below.

Where can the administrator check for more information on these errors?



- A. The Log and Monitor section in SmartConsole
- B. The Validations section in SmartConsole
- C. The Objects section in SmartConsole
- D. The Policies section in SmartConsole

Answer: B

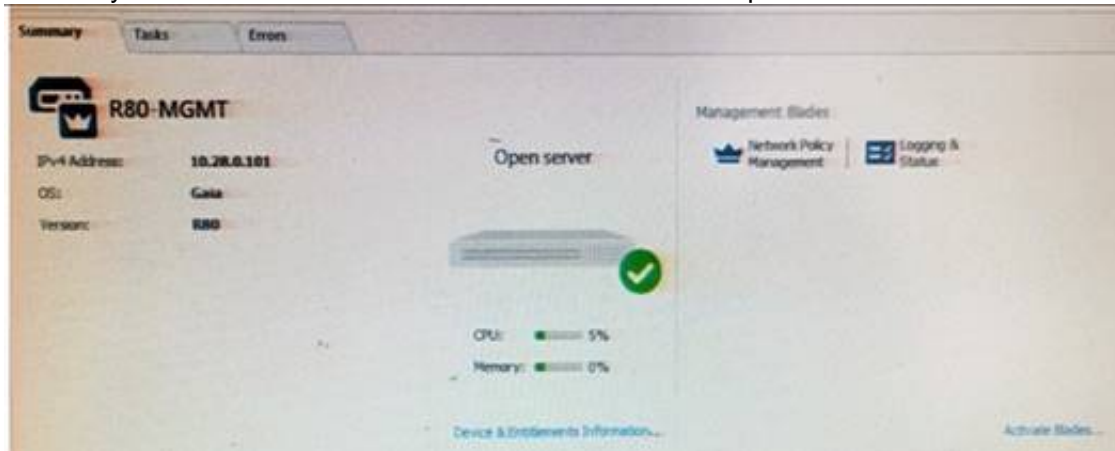
Explanation: Validation Errors

The validations pane in SmartConsole shows configuration error messages. Examples of errors are object names that are not unique, and the use of objects that are not valid in the Rule Base.

To publish, you must fix the errors.

NEW QUESTION 160

Tina is a new administrator who is currently reviewing the new Check Point R80 Management console interface. In the Gateways view, she is reviewing the Summary screen as in the screenshot below. What is an 'Open Server'?



- A. Check Point software deployed on a non-Check Point appliance.
- B. The Open Server Consortium approved Server Hardware used for the purpose of Security and Availability.
- C. A Check Point Management Server deployed using the Open Systems Interconnection (OSI) Server and Security deployment model.
- D. A Check Point Management Server software using the Open SSL.

Answer: A

Explanation:

Open Server	Non-Check Point hardware platform that is certified by Check Point as supporting Check Point products. Open Servers allow customers the flexibility of deploying Check Point software on systems which have not been pre-hardened or pre-installed (servers running standard versions of Solaris, Windows, Red Hat Linux).
--------------------	--

Topic 2, Exam Pool B

NEW QUESTION 163

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 165

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 167

Which of the following is NOT an element of VPN Simplified Mode and VPN Communities?

- A. "Encrypt" action in the Rule Base
- B. Permanent Tunnels
- C. "VPN" column in the Rule Base
- D. Configuration checkbox "Accept all encrypted traffic"

Answer: A

Explanation: Migrating from Traditional Mode to Simplified Mode

To migrate from Traditional Mode VPN to Simplified Mode:

1. On the Global Properties > VPN page, select one of these options:

- Simplified mode to all new Firewall Policies
- Traditional or Simplified per new Firewall Policy

2. Click OK.

3. From the R80 SmartConsole Menu, select Manage policies. The Manage Policies window opens.

4. Click New.

The New Policy window opens.

5. Give a name to the new policy and select Access Control.

In the Security Policy Rule Base, a new column marked VPN shows and the Encrypt option is no longer available in the Action column. You are now working in Simplified Mode.

NEW QUESTION 172

In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?

- A. Rule 0
- B. Blank field under Rule Number
- C. Rule 1
- D. Cleanup Rule

Answer: A

NEW QUESTION 175

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 180

What are the three tabs available in SmartView Tracker?

- A. Network & Endpoint, Management, and Active
- B. Network, Endpoint, and Active
- C. Predefined, All Records, Custom Queries
- D. Endpoint, Active, and Custom Queries

Answer: C

NEW QUESTION 183

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

- A. RADIUS
- B. Remote Access and RADIUS
- C. AD Query
- D. AD Query and Browser-based Authentication

Answer: D

Explanation: Identity Awareness gets identities from these acquisition sources:

AD Query

Browser-Based Authentication

Endpoint Identity Agent

Terminal Servers Identity Agent

Remote Access

NEW QUESTION 184

Can a Check Point gateway translate both source IP address and destination IP address in a given packet?

- A. Yes.
- B. No.
- C. Yes, but only when using Automatic NAT.
- D. Yes, but only when using Manual NAT.

Answer: A

NEW QUESTION 189

Where do we need to reset the SIC on a gateway object?

- A. SmartDashboard > Edit Gateway Object > General Properties > Communication
- B. SmartUpdate > Edit Security Management Server Object > SIC
- C. SmartUpdate > Edit Gateway Object > Communication

D. SmartDashboard > Edit Security Management Server Object > SIC

Answer: A

NEW QUESTION 194

Which of the following is NOT an alert option?

- A. SNMP
- B. High alert
- C. Mail
- D. User defined alert

Answer: B

Explanation: In Action, select:

none - No alert.

log - Sends a log entry to the database.

alert - Opens a pop-up window to your desktop.

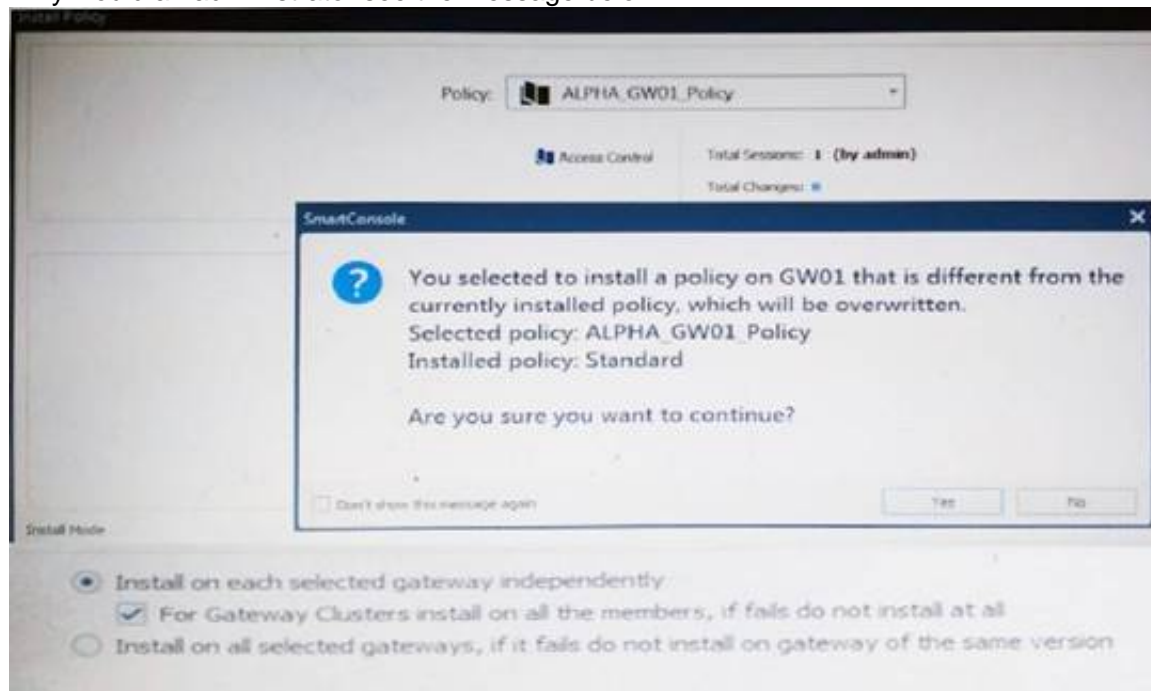
mail - Sends a mail alert to your Inbox.

snmptrap - Sends an SNMP alert.

useralert - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert > Alert Commands.

NEW QUESTION 198

Why would an administrator see the message below?

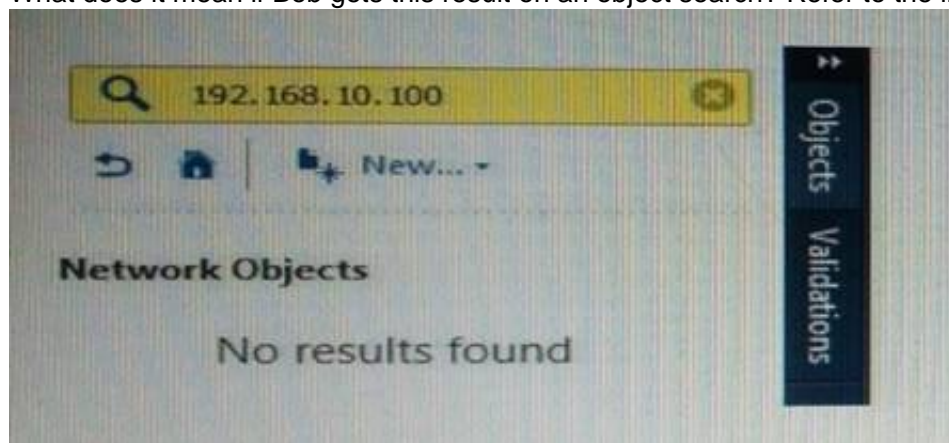


- A. A new Policy Package created on both the Management and Gateway will be deleted and must be packed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed 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 202

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 204

Which of the following is NOT an advantage to using multiple LDAP servers?

- A. You achieve a faster access time by placing LDAP servers containing the database at remote sites
- B. Information on a user is hidden, yet distributed across several servers
- C. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
- D. You gain High Availability by replicating the same information on several servers

Answer: B

NEW QUESTION 207

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.

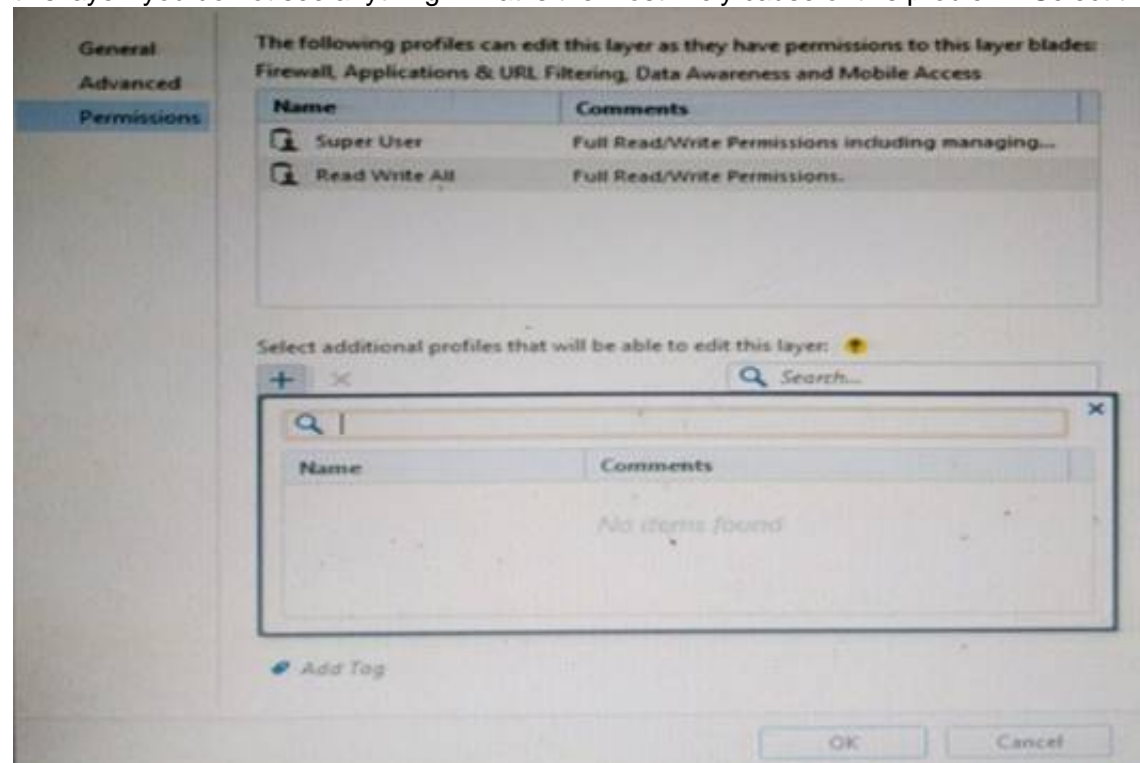
Snapshot (Revert)

Backup (Restore)

upgrade_export (Migrate) References:

NEW QUESTION 211

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 213

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, gateway policy permits access only from John's desktop which is assigned an IP address 10.0.0.19 via DHCP.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but the limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to move around the organization and continue to have access to the HR Web Server. To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

- A. John should install the identity Awareness Agent
- B. The firewall admin should install the Security Policy
- C. John should lock and unlock the computer
- D. Investigate this as a network connectivity issue

Answer: C

NEW QUESTION 217

Which of the following is TRUE about the Check Point Host object?

- A. Check Point Host has no routing ability even if it has more than one interface installed.
- B. When you upgrade to R80 from R77.30 or earlier versions, Check Point Host objects are converted to gateway objects.
- C. Check Point Host is capable of having an IP forwarding mechanism.
- D. Check Point Host can act as a firewall.

Answer: A

Explanation: A Check Point host is a host with only one interface, on which Check Point software has been installed, and which is managed by the Security Management server. It is not a routing mechanism and is not capable of IP forwarding.

NEW QUESTION 220

Fill in the blank: The ____ software blade enables Application Security policies to allow, block, or limit website access based on user, group, and machine identities.

- A. Application Control
- B. Data Awareness
- C. URL Filtering
- D. Threat Emulation

Answer: A

NEW QUESTION 222

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 223

MyCorp has the following NAT rules. You need to disable the NAT function when Alpha-internal networks try to reach the Google DNS (8.8.8.8) server. What can you do in this case?

- A. Use manual NAT rule to make an exception
- B. Use the NAT settings in the Global Properties
- C. Disable NAT inside the VPN community
- D. Use network exception in the Alpha-internal network object

Answer: D

NEW QUESTION 224

Fill in the blank: A(n) ____ rule is created by an administrator and is located before the first and before last rules in the Rule Base.

- A. Firewall drop
- B. Explicit
- C. Implicit accept
- D. Implicit drop
- E. Implied

Answer: E

Explanation: This is the order that rules are enforced:

First Implied Rule: You cannot edit or delete this rule and no explicit rules can be placed before it.

Explicit Rules: These are rules that you create.

Before Last Implied Rules: These implied rules are applied before the last explicit rule.

Last Explicit Rule: We recommend that you use the Cleanup rule as the last explicit rule.

Last Implied Rules: Implied rules that are configured as Last in Global Properties.

Implied Drop Rule: Drops all packets without logging.

NEW QUESTION 229

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 230

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 235

Study the Rule base and Client Authentication Action properties screen.

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

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 240

Which Check Point software blade prevents malicious files from entering a network using virus signatures and anomaly-based protections from ThreatCloud?

- A. Firewall
- B. Application Control
- C. Anti-spam and Email Security
- D. Antivirus

Answer: D

Explanation: The enhanced Check Point Antivirus Software Blade uses real-time virus signatures and anomaly-based protections from ThreatCloud™, the first collaborative network to fight cybercrime, to detect and block malware at the gateway before users are affected.

NEW QUESTION 241

Office mode means that:

- A. SecureID client assigns a routable MAC address
- B. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
- C. Users authenticate with an Internet browser and use secure HTTPS connection.
- D. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
- E. Allows a security gateway to assign a remote client an IP address
- F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

Explanation: Office Mode enables a Security Gateway to assign internal IP addresses to SecureClient users. This IP address will not be exposed to the public network, but is encapsulated inside the VPN tunnel between the client and the Gateway. The IP to be used externally should be assigned to the client in the usual way by the Internet Service provider used for the Internet connection. This mode allows a Security Administrator to control which addresses are used by remote clients inside the local network and makes them part of the local network. The mechanism is based on an IKE protocol extension through which the Security Gateway can send an internal IP address to the client.

NEW QUESTION 246

Joey is using the computer with IP address 192.168.20.13. He wants to access web page “www.Check Point.com”, which is hosted on Web server with IP address 203.0.113.111. How many rules on Check Point Firewall are required for this connection?

- A. Two rules – first one for the HTTP traffic and second one for DNS traffic.
- B. Only one rule, because Check Point firewall is a Packet Filtering firewall
- C. Two rules – one for outgoing request and second one for incoming replay.
- D. Only one rule, because Check Point firewall is using Stateful Inspection technology.

Answer: D

NEW QUESTION 248

Which Check Point software blade provides visibility of users, groups and machines while also providing access control through identity-based policies?

- A. Firewall
- B. Identity Awareness
- C. Application Control
- D. URL Filtering

Answer: B

Explanation: Check Point Identity Awareness Software Blade provides granular visibility of users, groups and machines, providing unmatched application and access control through the creation of accurate, identity-based policies. Centralized management and monitoring allows for policies to be managed from a single, unified console.

NEW QUESTION 253

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 clickUpdate Now.

NEW QUESTION 255

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.
- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server

Answer: D

Explanation: Users

Use the WebUI and CLI to manage user accounts. You can:

Add users to your Gaia system.

Edit the home directory of the user.

Edit the default shell for a user.

Give a password to a user.

Give privileges to users.

NEW QUESTION 260

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 263

Bob and Joe both have Administrator Roles on their Gaia Platform. Bob logs in on the WebUI and then Joe logs in through CLI. Choose what BEST describes the following scenario, where Bob and Joe are both logged in:

- A. When Joe logs in, Bob will be log out automatically.
- B. Since they both are log in on different interfaces, they both will be able to make changes.
- C. If Joe tries to make changes, he won't, database will be locked.
- D. Bob will be prompt that Joe logged in.

Answer: C

NEW QUESTION 265

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

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

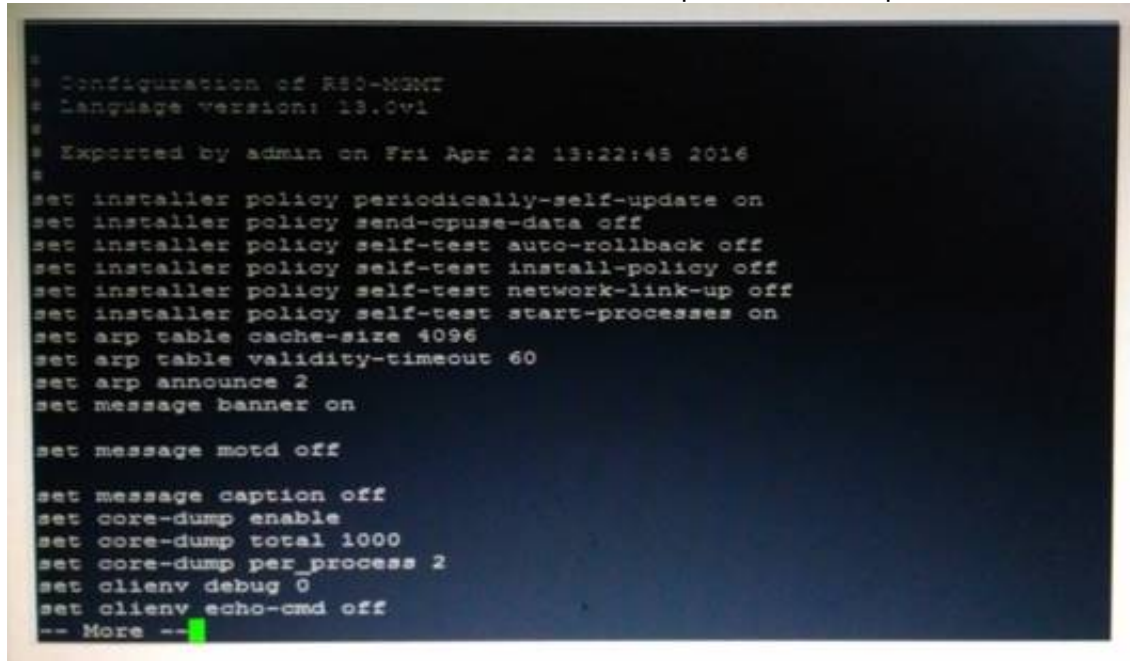
Answer: C

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 267

Look at the screenshot below. What CLISH command provides this output?



```
* Configuration of R80-MGMT
* Language version: 13.0v1
*
* Exported by admin on Fri Apr 22 13:22:45 2016
*
set installer policy periodically-self-update on
set installer policy send-cpuse-data off
set installer policy self-test auto-rollback off
set installer policy self-test install-policy off
set installer policy self-test network-link-up off
set installer policy self-test start-processes on
set arp table cache-size 4096
set arp table validity-timeout 60
set arp announce 2
set message banner on

set message motd off

set message caption off
set core-dump enable
set core-dump total 1000
set core-dump per_process 2
set clienv debug 0
set clienv echo-cmd off
-- More --
```

- A. show configuration all
- B. show confd configuration
- C. show confd configuration all
- D. show configuration

Answer: D

NEW QUESTION 272

What is the default method for destination NAT?

- A. Destination side
- B. Source side
- C. Server side
- D. Client side

Answer: D

NEW QUESTION 273

Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _____.

- A. Firewall policy install
- B. Threat Prevention policy install
- C. Anti-bot policy install
- D. Access Control policy install

Answer: B

Explanation: https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 276

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 280

NAT can NOT be configured on which of the following objects?

- A. HTTP Logical Server
- B. Gateway
- C. Address Range
- D. Host

Answer: A

NEW QUESTION 281

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 283

Where can administrator edit a list of trusted SmartConsole clients in R80?

- A. cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server.
- B. Only using SmartConsole: Manage and Settings > Permissions and Administrators > Advanced > Trusted Clients.
- C. In cpconfig on a Security Management Server, in the WebUI logged into a Security Management Server, in SmartConsole: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients.
- D. WebUI client logged to Security Management Server, SmartDashboard: Manage and Settings>Permissions and Administrators>Advanced>Trusted Clients, via cpconfig on a Security Gateway.

Answer: C

NEW QUESTION 286

Which command is used to obtain the configuration lock in Gaia?

- A. Lock database override
- B. Unlock database override
- C. Unlock database lock
- D. Lock database user

Answer: A

Explanation: Obtaining a Configuration Lock

lock database override
unlock database

NEW QUESTION 289

The IT Management team is interested in the new features of the Check Point R80 Management and wants to upgrade but they are concerned that the existing R77.30 Gaia Gateways cannot be managed by R80 because it is so different. As the administrator responsible for the Firewalls, how can you answer or confirm these concerns?

A. R80 Management contains compatibility packages for managing earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.

- B. R80 Management requires the separate installation of compatibility hotfix packages for managing the earlier versions of Check Point Gateways prior to R80. Consult the R80 Release Notes for more information.
- C. R80 Management was designed as a completely different Management system and so can only monitor Check Point Gateways prior to R80.
- D. R80 Management cannot manage earlier versions of Check Point Gateways prior to R80. Only R80 and above Gateways can be manage
- E. Consult the R80 Release Notes for more information.

Answer: A

NEW QUESTION 290

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 293

In the R80 SmartConsole, on which tab are Permissions and Administrators defined?

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

Answer: C

NEW QUESTION 295

Which of the following statements accurately describes the command snapshot?

- A. snapshot creates a full OS-level backup, including network-interface data, Check Point production information, and configuration settings of a GAiA Security Gateway.
- B. snapshot creates a Security Management Server full system-level backup on any OS
- C. snapshot stores only the system-configuration settings on the Gateway
- D. A Gateway snapshot includes configuration settings and Check Point product information from the remote Security Management Server

Answer: A

NEW QUESTION 299

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 300

Which of the following licenses are considered temporary?

- A. Perpetual and Trial
- B. Plug-and-play and Evaluation
- C. Subscription and Perpetual
- D. Evaluation and Subscription

Answer: B

Explanation: Should be Trial or Evaluation, even Plug-and-play (all are synonyms). Answer B is the best choice.

NEW QUESTION 302

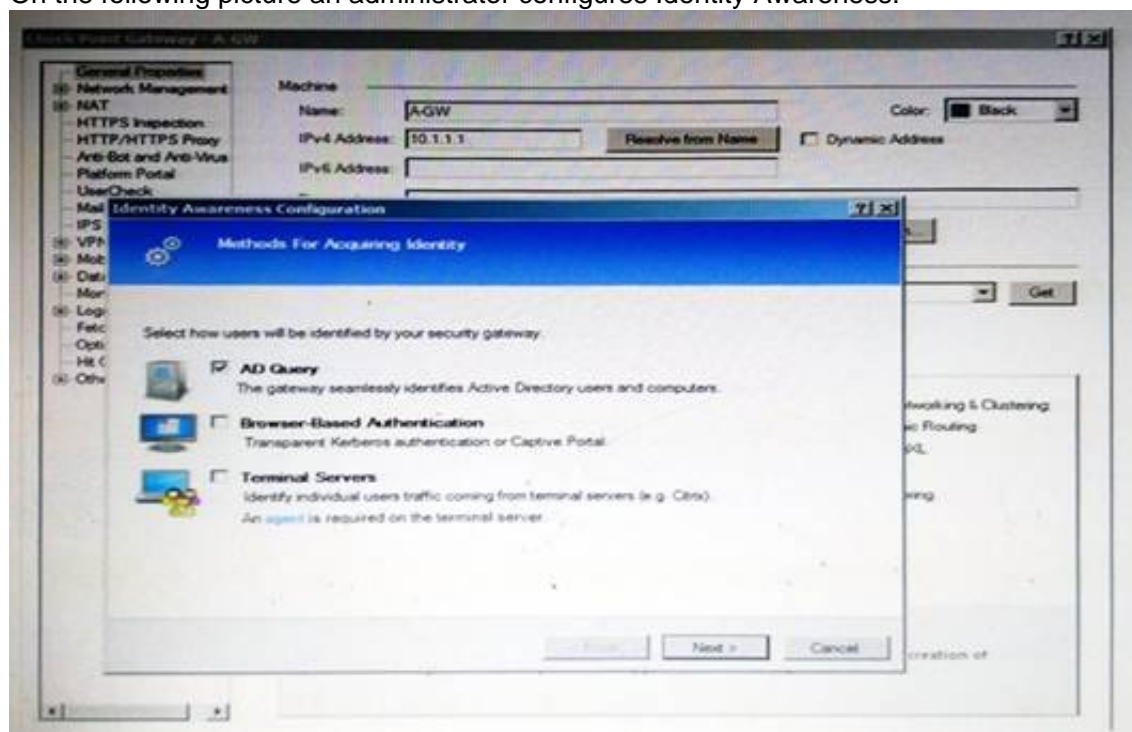
AdminA and AdminB are both logged in on SmartConsole. What does it mean if AdminB sees a locked icon on a rule? Choose the BEST answer.

- A. Rule is locked by AdminA, because the save bottom has not been press.
- B. Rule is locked by AdminA, because an object on that rule is been edited.
- C. Rule is locked by AdminA, and will make it available if session is published.
- D. Rule is locked by AdminA, and if the session is saved, rule will be available

Answer: C

NEW QUESTION 307

On the following picture an administrator configures Identity Awareness:



After clicking “Next” the above configuration is supported by:

- A. Kerberos SSO which will be working for Active Directory integration
- B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user
- C. Obligatory usage of Captive Portal
- D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication

Answer: B

Explanation: To enable Identity Awareness:

Log in to R80 SmartConsole.

From the Awareness.

Gateway&s

Servers

view, double-click the Security Gateway on which to enable Identity

On the Network Security tab, select Identity Awareness.

The Identity Awareness

Configuration wizard opens.

Select one or more options. These options set the methods for acquiring identities of managed and unmanaged assets.

AD Query - Lets the Security Gateway seamlessly identify Active Directory users and computers

Browser-Based Authentication - Sends users to a Web page to acquire identities from unidentified users. If Transparent Kerberos Authentication is configured, AD users may be identified transparently.

Terminal Servers - Identify users in a Terminal Server environment (originating from one IP address).

NEW QUESTION 311

Your bank's distributed R77 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

- A. SmartView Tracker
- B. SmartPortal
- C. SmartUpdate
- D. SmartDashboard

Answer: C

NEW QUESTION 316

Which type of Endpoint Identity Agent includes packet tagging and computer authentication?

- A. Full
- B. Light
- C. Custom
- D. Complete

Answer: A

Explanation: Endpoint Identity Agents – dedicated client agents installed on users' computers that acquire and report identities to the Security Gateway.

NEW QUESTION 318

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 322

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.

Topic 3, Exam Pool C

NEW QUESTION 324

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

- A. Threat Emulation
- B. Mobile Access
- C. Mail Transfer Agent
- D. Threat Cloud

Answer: C

NEW QUESTION 326

In what way are SSL VPN and IPSec VPN different?

- A. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
- B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
- C. IPSec VPN does not support two factor authentication, SSL VPN does support this
- D. IPSec VPN uses an additional virtual adapter, SSL VPN uses the client network adapter only

Answer: D

NEW QUESTION 330

Which limitation of CoreXL is overcome by using (mitigated by) Multi-Queue?

- A. There is no traffic queue to be handled
- B. Several NICs can use one traffic queue by one CPU
- C. Each NIC has several traffic queues that are handled by multiple CPU cores
- D. Each NIC has one traffic queue that is handled by one CPU

Answer: C

NEW QUESTION 334

As you review this Security Policy, what changes could you make to accommodate Rule 4?

No.	Hits	Name	Source	Destination	VPN	Service	Action
Limit Access to Gateways (Rule 1)							
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
VPN Access Rules (Rules 2-5)							
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth.
5	0	Web Server	L2TP-vpn-user@Any Customers@Any	Remote-1-web-server	Any Traffic	http	accept

- A. Remove the service HTTP from the column Service in Rule 4.

- B. Modify the column VPN in Rule 2 to limit access to specific traffic.
- C. Nothing at all
- D. Modify the columns Source or Destination in Rule 4

Answer: B

NEW QUESTION 337

Where do you verify that UserDirectory is enabled?

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

Answer: D

NEW QUESTION 341

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 342

The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

- A. Secure Internal Communication (SIC)
- B. Restart Daemons if they fail
- C. Transfer messages between Firewall processes
- D. Pulls application monitoring status

Answer: D

NEW QUESTION 344

Your boss wants you to closely monitor an employee suspected of transferring company secrets to the competition. The IT department discovered the suspect installed a WinSCP client in order to use encrypted communication. Which of the following methods is BEST to accomplish this task?

- A. Use SmartView Tracker to follow his actions by filtering log entries that feature the WinSCP destination port
- B. Then, export the corresponding entries to a separate log file for documentation.
- C. Use SmartDashboard to add a rule in the firewall Rule Base that matches his IP address, and those of potential targets and suspicious protocol
- D. Apply the alert action or customized messaging.
- E. Watch his IP in SmartView Monitor by setting an alert action to any packet that matches your Rule Base and his IP address for inbound and outbound traffic.
- F. Send the suspect an email with a keylogging Trojan attached, to get direct information about his wrongdoings.

Answer: A

NEW QUESTION 348

Which of the below is the MOST correct process to reset SIC from SmartDashboard?

- A. Run cpconfig, and click Reset.
- B. Click the Communication button for the firewall object, then click Reset
- C. Run cpconfig on the gateway and type a new activation key.
- D. Run cpconfig, and select Secure Internal Communication > Change One Time Password.
- E. Click Communication > Reset on the Gateway object, and type a new activation key.

Answer: B

NEW QUESTION 353

Choose the correct statement regarding Implicit Rules.

- A. To edit the Implicit rules you go to: Launch Button > Policy > Global Properties > Firewall.
- B. Implied rules are fixed rules that you cannot change.
- C. You can directly edit the Implicit rules by double-clicking on a specific Implicit rule.
- D. You can edit the Implicit rules but only if requested by Check Point support personnel.

Answer: A

NEW QUESTION 356

An internal router is sending UDP keep-alive packets that are being encapsulated with GRE and sent through your R77 Security Gateway to a partner site. A rule for GRE traffic is configured for ACCEPT/LOG. Although the keep-alive packets are being sent every minute, a search through the SmartView Tracker logs for GRE traffic only shows one entry for the whole day (early in the morning after a Policy install).

Your partner site indicates they are successfully receiving the GRE encapsulated keep-alive packets on the 1-minute interval. If GRE encapsulation is turned off on the router, SmartView Tracker shows a log entry for the UDP keep-alive packet every minute. Which of the following is the BEST Explanation: for this behavior?

- A. The setting Log does not capture this level of detail for GR
- B. Set the rule tracking action to Audit since certain types of traffic can only be tracked this way.
- C. The log unification process is using a LUUID (Log Unification Unique Identification) that has become corrup
- D. Because it is encrypted, the R77 Security Gateway cannot distinguish between GRE session
- E. This is a known issue with GR
- F. Use IPSEC instead of the non-standard GRE protocol for encapsulation.
- G. The Log Server log unification process unifies all log entries from the Security Gateway on a specific connection into only one log entry in the SmartView Tracker
- H. GRE traffic has a 10 minute session timeout, thus each keep-alive packet is considered part of the original logged connection at the beginning of the day.
- I. The Log Server is failing to log GRE traffic properly because it is VPN traffi
- J. Disable all VPN configuration to the partner site to enable proper logging.

Answer: C

NEW QUESTION 357

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 362

How many packets does the IKE exchange use for Phase 1 Main Mode?

- A. 12
- B. 1
- C. 3
- D. 6

Answer: D

NEW QUESTION 365

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 370

Which rule is responsible for the user authentication failure?

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
1	0	NetBIOS	Any	Any	Any Traffic	NBT	drop	None
2	0	Management	webSingapore	fwSingapore	Any Traffic	ssh https	accept	None
3	0	Stealth	Any	fwSingapore	Any Traffic	Any	drop	Log
4	0	User Auth	Any	webSingapore	Any Traffic	http	User Auth	Log
5	0	Partner City	net_singapore net_rome net_singapore net_singapore net_sydney	net_rome net_singapore	rome_singapore	http	accept	Log
6	0	Network Traffic		Any	Any Traffic	http dns icmp-proto ftp https	accept	Log
7	0	Cleanup	Any	Any	Any Traffic	Any	drop	Log

- A. Rule 4
- B. Rule 6
- C. Rule 3
- D. Rule 5

Answer: C

NEW QUESTION 375

How do you configure the Security Policy to provide uses access to the Captive Portal through an external (Internet) interface?

- A. Change the gateway settings to allow Captive Portal access via an external interface.
- B. No action is necessar
- C. This access is available by default.
- D. Change the Identity Awareness settings under Global Properties to allow Captive Policy access on all interfaces.
- E. Change the Identity Awareness settings under Global Properties to allow Captive Policy access for an external interface.

Answer: A

NEW QUESTION 376

To fully enable Dynamic Dispatcher on a Security Gateway:

- A. run fw ctl multik set_mode 9 in Expert mode and then reboot
- B. Using cpconfig, update the Dynamic Dispatcher value to “full” under the CoreXL menu
- C. Edit /proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot
- D. run fw ctl multik set_mode 1 in Expert mode and then reboot

Answer: A

NEW QUESTION 381

Which of these statements describes the Check Point ThreatCloud?

- A. Blocks or limits usage of web applications
- B. Prevents or controls access to web sites based on category
- C. Prevents Cloud vulnerability exploits
- D. A worldwide collaborative security network

Answer: D

NEW QUESTION 382

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 387

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

Command	Function
C1 cp_admin_convert	F1: export and import different revisions of the database.
C2 cpca_client	F2: export and import policy package
C3 cp_merge	F3: transfer Log data to an external database.
C4 cpwd_admin	F4: execute operations on the ICA.
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in cpconfig to SmartDashboard.

- 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 391

You manage a global network extending from your base in Chicago to Tokyo, Calcutta and Dallas. Management wants a report detailing the current software level of each Enterprise class Security Gateway. You plan to take the opportunity to create a proposal outline, listing the most cost-effective way to upgrade your Gateways. Which two SmartConsole applications will you use to create this report and outline?

- A. SmartView Tracker and SmartView Monitor
- B. SmartLSM and SmartUpdate
- C. SmartDashboard and SmartView Tracker
- D. SmartView Monitor and SmartUpdate

Answer: D

NEW QUESTION 392

Review the rules. Assume domain UDP is enabled in the implied rules.

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

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 397

Which remote Access Solution is clientless?

- A. Checkpoint Mobile
- B. Endpoint Security Suite
- C. SecuRemote
- D. Mobile Access Portal

Answer: D

NEW QUESTION 402

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

- A. Install appliance TE250X on SpanPort on LAN switch in MTA mode
- B. Install appliance TE250X in standalone mode and setup MTA
- C. You can utilize only Check Point Cloud Services for this scenario
- D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance

Answer: C

NEW QUESTION 403

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 405

Which of the following uses the same key to decrypt as it does to encrypt?

- A. Asymmetric encryption
- B. Dynamic encryption
- C. Certificate-based encryption
- D. Symmetric encryption

Answer: D

NEW QUESTION 410

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his desktop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.
- 3) Changes from static IP address to DHCP for the client PC.

What should John request when he cannot access the web server from his laptop?

- A. John should lock and unlock his computer
- B. Investigate this as a network connectivity issue
- C. The access should be changed to authenticate the user instead of the PC
- D. John should install the Identity Awareness Agent

Answer: C

NEW QUESTION 413

Which the following type of authentication on Mobile Access can NOT be used as the first authentication method?

- A. Dynamic ID
- B. RADIUS
- C. Username and Password
- D. Certificate

Answer: A

NEW QUESTION 416

A client has created a new Gateway object that will be managed at a remote location. When the client attempts to install the Security Policy to the new Gateway object, the object does not appear in the Install On check box. What should you look for?

- A. Secure Internal Communications (SIC) not configured for the object.
- B. A Gateway object created using the Check Point > Externally Managed VPN Gateway option from the Network Objects dialog box.
- C. Anti-spoofing not configured on the interfaces on the Gateway object.
- D. A Gateway object created using the Check Point > Secure Gateway option in the network objects, dialog box, but still needs to configure the interfaces for the Security Gateway object.

Answer: B

NEW QUESTION 421

During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

- A. Dropped without sending a negative acknowledgment
- B. Dropped without logs and without sending a negative acknowledgment
- C. Dropped with negative acknowledgment
- D. Dropped with logs and without sending a negative acknowledgment

Answer: D

NEW QUESTION 422

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 426

What is Consolidation Policy?

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

Answer: B

NEW QUESTION 431

As a Security Administrator, you must refresh the Client Authentication authorized time-out every time a new user connection is authorized. How do you do this? Enable the Refreshable Timeout setting:

- A. in the user object's Authentication screen.
- B. in the Gateway object's Authentication screen.
- C. in the Limit tab of the Client Authentication Action Properties screen.
- D. in the Global Properties Authentication screen.

Answer: C

NEW QUESTION 432

You find that Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Choose the BEST reason why.

- A. You checked the cache password on desktop option in Global Properties.
- B. Another rule that accepts HTTP without authentication exists in the Rule Base.
- C. You have forgotten to place the User Authentication Rule before the Stealth Rule.
- D. Users must use the SecuRemote Client, to use the User Authentication Rule.

Answer: B

NEW QUESTION 436

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 441

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?

URL List Version	<input type="checkbox"/>	100
Unreachable directories	<input type="checkbox"/>	100
Update Service	<input type="checkbox"/>	100
Update Source	<input type="checkbox"/>	100
Update Status	<input type="checkbox"/>	100
User Action Comment	<input type="checkbox"/>	100
User Additional Information	<input type="checkbox"/>	100
User Check	<input type="checkbox"/>	100
User DN	<input type="checkbox"/>	100
User Directory	<input type="checkbox"/>	100
User Display Name	<input type="checkbox"/>	100
User Group	<input type="checkbox"/>	100
User Reported Wrong Category	<input type="checkbox"/>	100
User Response	<input type="checkbox"/>	100
User SID	<input type="checkbox"/>	100
User UID	<input type="checkbox"/>	100
User's IP	<input type="checkbox"/>	100
UserCheck ID	<input type="checkbox"/>	100
UserCheck Interaction Name	<input type="checkbox"/>	100
UserCheck Message to User	<input type="checkbox"/>	100
UserCheck Scope	<input type="checkbox"/>	100
UserCheck User Input	<input type="checkbox"/>	100
VLAN ID	<input type="checkbox"/>	100
VPN Feature	<input type="checkbox"/>	100
VPN Peer Gateway	<input type="checkbox"/>	100
Version	<input type="checkbox"/>	100
Virtual Link	<input type="checkbox"/>	100
Virus Name	<input type="checkbox"/>	100
VoIP Duration	<input type="checkbox"/>	100
VoIP Log Type	<input type="checkbox"/>	100
VoIP Reject Reason	<input type="checkbox"/>	100
VoIP Reject Reason Information	<input type="checkbox"/>	100
Web Filtering Categories	<input type="checkbox"/>	100
Wire Byte/Sec Out	<input type="checkbox"/>	100
Wire Byte/Sec in	<input type="checkbox"/>	100
Wire Packet/Sec Out	<input type="checkbox"/>	100
Wire Packet/Sec in	<input type="checkbox"/>	100
Write Access	<input type="checkbox"/>	100
XlateDPort	<input type="checkbox"/>	100
XlateDst	<input type="checkbox"/>	100
XlateSPort	<input type="checkbox"/>	100
XlateSrc	<input type="checkbox"/>	100
Special properties	<input type="checkbox"/>	100

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

Answer: B

NEW QUESTION 446

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 448

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 453

Where would an administrator enable Implied Rules logging?

- A. In Smart Log Rules View
- B. In SmartDashboard on each rule
- C. In Global Properties under Firewall
- D. In Global Properties under log and alert

Answer: B

NEW QUESTION 456

Which of the following is NOT an attribute of packer acceleration?

- A. Source address
- B. Protocol
- C. Destination port
- D. Application Awareness

Answer: D

NEW QUESTION 459

MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. How do you apply the license?

- A. Using the remote Gateway's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- B. Using your Security Management Server's IP address, and attaching the license to the remote Gateway via SmartUpdate.
- C. Using the remote Gateway's IP address, and applying the license locally with command cplic put.
- D. Using each of the Gateway's IP addresses, and applying the licenses on the Security Management Server with the command cprlic put.

Answer: B

NEW QUESTION 461

According to Check Point Best Practice, when adding a non-managed Check Point Gateway to a Check Point security solution what object SHOULD be added? A(n):

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

Answer: C

NEW QUESTION 463

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 466

Which NAT rules are prioritized first?

- A. Post-Automatic/Manual NAT rules
- B. Manual/Pre-Automatic NAT
- C. Automatic Hide NAT
- D. Automatic Static NAT

Answer: B

NEW QUESTION 468

What is the appropriate default Gaia Portal address?

- A. HTTP://[IPADDRESS]
- B. HTTPS://[IPADDRESS]:8080
- C. HTTPS://[IPADDRESS]:4434
- D. HTTPS://[IPADDRESS]

Answer: D

NEW QUESTION 473

When launching SmartDashboard, what information is required to log into R77?

- A. User Name, Management Server IP, certificate fingerprint file
- B. User Name, Password, Management Server IP
- C. Password, Management Server IP
- D. Password, Management Server IP, LDAP Server IP

Answer: B

NEW QUESTION 476

What is the benefit of Manual NAT over Automatic NAT?

- A. If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy
- B. There is no benefit since Automatic NAT has in any case higher priority over Manual NAT
- C. You have the full control about the priority of the NAT rules
- D. On IPSO and GAIA Gateways, it is handled in a Stateful manner

Answer: C

NEW QUESTION 479

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 480

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

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

Answer: A

NEW QUESTION 483

When using GAiA, it might be necessary to temporarily change the MAC address of the interface eth 0 to 00:0C:29:12:34:56. After restarting the network the old MAC address should be active. How do you configure this change?

- A. As expert user, issue these commands:# IP link set eth0 down# IP link set eth0 addr 00:0C:29:12:34:56# IP link set eth0 up
- B. Edit the file /etc/sysconfig/netconf.C and put the new MAC address in the field(conf:(conns:(conn:hwaddr ("00:0C:29:12:34:56"))
- C. As expert user, issue the command:# IP link set eth0 addr 00:0C:29:12:34:56
- D. Open the WebUI, select Network > Connections > eth0. Place the new MAC address in the field Physical Address, and press Apply to save the settings.

Answer: C

NEW QUESTION 487

Identify the API that is not supported by Check Point currently.

- A. R80 Management API-
- B. Identity Awareness Web Services API
- C. Open REST API
- D. OPSEC SDK

Answer: C

NEW QUESTION 489

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 491

If the first packet of an UDP session is rejected by a security policy, what does the firewall send to the client?

- A. Nothing
- B. TCP FIN
- C. TCP RST
- D. ICMP unreachable

Answer: A

NEW QUESTION 494

What happens when you run the command: fw sam -J src [Source IP Address]?

- A. Connections from the specified source are blocked without the need to change the Security Policy.
- B. Connections to the specified target are blocked without the need to change the Security Policy.
- C. Connections to and from the specified target are blocked without the need to change the Security Policy.
- D. Connections to and from the specified target are blocked with the need to change the Security Policy.

Answer: A

NEW QUESTION 496

Which of the following commands is used to verify license installation?

- A. Cplic verify license
- B. Cplic print
- C. Cplic show
- D. Cplic license

Answer: B

NEW QUESTION 501

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 504

Tom has connected to the R80 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made:

- A. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of this work.
- B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- C. Tom's changes will be lost since he lost connectivity and he will have to start again.
- D. Tom will have to reboot his SmartConsole computer, clear the cache and restore changes.

Answer: A

NEW QUESTION 505

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 506

Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

- A. The rule base can be built of layers, each containing a set of the security rule
- B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- D. Time object to a rule to make the rule active only during specified times.
- E. Sub Policies are sets of rules that can be created and attached to specific rule
- F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 510

What is a reason for manual creation of a NAT rule?

- A. In R80 all Network Address Translation is done automatically and there is no need for manually defined NAT-rules.
- B. Network Address Translation of RFC1918-compliant networks is needed to access the Internet.

- C. Network Address Translation is desired for some services, but not for others.
D. The public IP-address is different from the gateway's external IP

Answer: D

NEW QUESTION 512

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 514

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 518

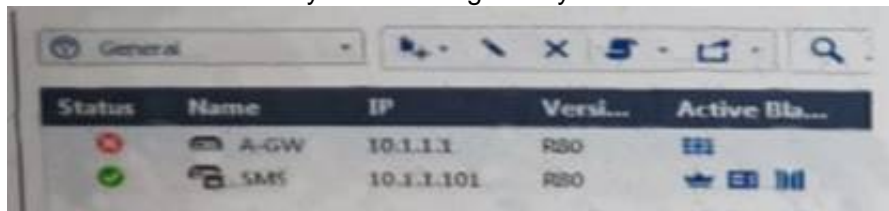
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

- A. Slow Path
B. Medium Path
C. Fast Path
D. Accelerated Path

Answer: A

NEW QUESTION 519

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 523

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 527

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265
B. TCP port 265
C. UDP port 256
D. TCP port 256

Answer: B

NEW QUESTION 532

From SecureXL perspective, what are the tree paths of traffic flow:

- A. Initial Path; Medium Path; Accelerated Path
- B. Layer Path; Blade Path; Rule Path
- C. Firewall Path; Accept Path; Drop Path
- D. Firewall Path; Accelerated Path; Medium Path

Answer: D

NEW QUESTION 537

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 538

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 539

The SmartEvent R80 Web application for real-time event monitoring is called:

- A. SmartView Monitor
- B. SmartEventWeb
- C. There is no Web application for SmartEvent
- D. SmartView

Answer: B

NEW QUESTION 543

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.

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NT	Drop	- None	Policy Targets
2	Management	Net_10.28.0.0	GW-87730	* Any	https, ssh	Accept	Log	Policy Targets
3	Stealth	* Any	GW-87730	* Any	* Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	* Any	Accept	Log	Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http, https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	Accept	Log	Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	Policy Targets

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 548

Of all the Check Point components in your network, which one changes most often and should be backed up most frequently?

- A. SmartManager
- B. SmartConsole
- C. Security Gateway
- D. Security Management Server

Answer: C

NEW QUESTION 550

Which back up utility captures the most information and tends to create the largest archives?

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

Answer: B

NEW QUESTION 551

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 555

Fill in the blank: In Security Gateways R75 and above, SIC uses _____ for encryption.

- A. AES-128
- B. AES-256
- C. DES
- D. 3DES

Answer: A

NEW QUESTION 556

Which is a suitable command to check whether Drop Templates are activated or not?

- A. fw ctl get int activate_drop_templates
- B. fwaccel stat
- C. fwaccel stats
- D. fw ctl templates -d

Answer: B

NEW QUESTION 561

When connected to the Check Point R80 Management Server using the SmartConsole the first administrator to connect has a lock on:

- A. Only the objects being modified in the Management Database and other administrators can connect to make changes using a special session as long as they all connect from the same LAN network.
- B. The entire Management Database and other administrators can connect to make changes only if the first administrator switches to Read-only.
- C. The entire Management Database and all sessions and other administrators can connect only as Read-only.
- D. Only the objects being modified in his session of the Management Database and other administrators can connect to make changes using different sessions.

Answer: D

NEW QUESTION 563

Can multiple administrators connect to a Security Management Server at the same time?

- A. No, only one can be connected
- B. Yes, all administrators can modify a network object at the same time
- C. Yes, every administrator has their own username, and works in a session that is independent of other administrators
- D. Yes, but only one has the right to write

Answer: C

NEW QUESTION 564

What is the Transport layer of the TCP/IP model responsible for?

- A. It transports packets as datagrams along different routes to reach their destination.
- B. It manages the flow of data between two hosts to ensure that the packets are correctly assembled and delivered to the target application.
- C. It defines the protocols that are used to exchange data between networks and how host programs interact with the Application layer.
- D. It deals with all aspects of the physical components of network connectivity and connects with different network types.

Answer: B

NEW QUESTION 565

The SIC Status "Unknown" means

- A. There is connection between the gateway and Security Management Server but it is not trusted.
- B. The secure communication is established.
- C. There is no connection between the gateway and Security Management Server.
- D. The Security Management Server can contact the gateway, but cannot establish SIC.

Answer: AC

Explanation: After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

Communicating - The secure communication is established.

Unknown - There is no connection between the gateway and Security Management Server.

Not Communicating - The Security Management Server can contact the gateway, but cannot establish SIC. A message shows more information.

NEW QUESTION 568

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 Seeting
- D. Security Policies

Answer: B

NEW QUESTION 569

How would you determine the software version from the CLI?

- A. fw ver
- B. fw stat
- C. fw monitor
- D. cpinfo

Answer: A

NEW QUESTION 573

Fill in the blank: By default, the SIC certificates issued by R80 Management Server are based on the _____ algorithm.

- A. SHA-256
- B. SHA-200
- C. MD5
- D. SHA-128

Answer: A

NEW QUESTION 574

SmartEvent does NOT use which of the following procedures to identity events:

- A. Matching a log against each event definition
- B. Create an event candidate
- C. Matching a log against local exclusions
- D. Matching a log against global exclusions

Answer: C

NEW QUESTION 575

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 577

Please choose correct command syntax to add an “emailserver1” host with IP address 10.50.23.90 using GAIa management CLI?

- A. host name myHost12 ip-address 10.50.23.90
- B. mgmt add host name ip-address 10.50.23.90
- C. add host name emailserver1 ip-address 10.50.23.90
- D. mgmt add host name emailserver1 ip-address 10.50.23.90

Answer: D

NEW QUESTION 580

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 582

When configuring LDAP User Directory integration, Changes applied to a User Directory template are:

- A. Reflected immediately for all users who are using template.
- B. Not reflected for any users unless the local user template is changed.
- C. Reflected for all users who are using that template and if the local user template is changed as well.
- D. Not reflected for any users who are using that template.

Answer: A

Explanation: The users and user groups are arranged on the Account Unit in the tree structure of the LDAP server. User management in User Directory is external, not local. You can change the User Directory templates. Users associated with this template get the changes immediately. You can change user definitions manually in SmartDashboard, and the changes are immediate on the server.

NEW QUESTION 586

Which command shows the installed licenses?

- A. cplic print
- B. print cplic
- C. fwlic print
- D. show licenses

Answer: A

NEW QUESTION 589

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 156-215.80 Exam with Our Prep Materials Via below:

<https://www.certleader.com/156-215.80-dumps.html>