

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

<https://www.2passeasy.com/dumps/156-215.81/>



NEW QUESTION 1

Name the file that is an electronically signed file used by Check Point to translate the features in the license into a code?

- A. Both License (.lic) and Contract (.xml) files
- B. cp.macro
- C. Contract file (.xml)
- D. license File (.lie)

Answer: B

Explanation:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 2

An administrator wishes to enable Identity Awareness on the Check Point firewalls. However they allow users to use company issued or personal laptops. Since the administrator cannot manage the personal laptops, which of the following methods would BEST suit this company?

- A. AD Query
- B. Browser-Based Authentication
- C. Identity Agents
- D. Terminal Servers Agent

Answer: B

NEW QUESTION 3

What is the purpose of the Stealth Rule?

- A. To prevent users from directly connecting to a Security Gateway.
- B. To reduce the number of rules in the database.
- C. To reduce the amount of logs for performance issues.
- D. To hide the gateway from the Internet.

Answer: A

NEW QUESTION 4





When URL Filtering is set, what identifying data gets sent to the Check Point Online Web Service?

- A. The URL and server certificate are sent to the Check Point Online Web Service
- B. The full URL, including page data, is sent to the Check Point Online Web Service
- C. The host part of the URL is sent to the Check Point Online Web Service
- D. The URL and IP address are sent to the Check Point Online Web Service

Answer: C

NEW QUESTION 5

What does it mean if Deyra sees the gateway status:

Status	Name	IP	Versi...	Active Bla...
	A-GW	10.1.1.1	R80	
	SMS	10.1.1.101	R80	  

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: B

Explanation:

fw-mini-ced
IP Address: **10.90.0.253**
Version: **R77.30**
OS: **Gaia Kernel Version: 2.6**
Up Time: **3 days and 4 hours**
[System Information](#), [Network Activity](#), [Licenses](#)

	Firewall	Security Policy: Standard_1 Installed On: Fri Dec 16 15:21:03 2016	More...
	ClusterXL	Working mode: High Availability (Active Up) Member state: active	More...
	IPSec VPN	Gateway to Gateway Tunnels: 0 Remote User Tunnels: 0	More...
	Identity Awareness	Error: At least one DC is currently disconnected	More...
	Mobile Access	Number of active sessions: 2	
	Anti-Bot & Anti-Virus	Anti-Bot subscription Status: Valid Anti-Bot subscription Expiration: Thu Jun 22 01:00:00 2017 Anti-Virus subscription Status: Valid Anti-Virus subscription Expiration: Thu Jun 22 01:00:00 2017	More...
	URL Filtering	Subscription Status: Valid Subscription Expiration: Thu Jun 22 01:00:00 2017	More...
	Application Control	Subscription Status: Valid Subscription Expiration: Thu Jun 22 01:00:00 2017	More...
	Anti-Spam		More...

NEW QUESTION 6

In a Distributed deployment, the Security Gateway and the Security Management software are installed on what platforms?

- A. Different computers or appliances.
- B. The same computer or appliance.
- C. Both on virtual machines or both on appliances but not mixed.
- D. In Azure and AWS cloud environments.

Answer: A

Explanation:

"The Security Management ServerClosed (1) and the Security GatewayClosed (3) are installed on different computers, with a network connection (2)."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 7

The Network Operations Center administrator needs access to Check Point Security devices mostly for troubleshooting purposes. You do not want to give her access to the expert mode, but she still should be able to run tcpdump. How can you achieve this requirement?

- A. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Create new user with any UID and assign role to the user.
- B. Add tcpdump to CLISH using add command.Create a new access role.Add tcpdump to the role.Createnew user with UID 0 and assign role to the user.
- C. Create a new access role.Add expert-mode access to the role.Create new user with UID 0 and assign role to the user.
- D. Create a new access role.Add expert-mode access to the role.Create new user with any UID and assign role to the user.

Answer: A

NEW QUESTION 8

Which statement is NOT TRUE about Delta synchronization?

- A. Using UDP Multicast or Broadcast on port 8161
- B. Using UDP Multicast or Broadcast on port 8116
- C. Quicker than Full sync
- D. Transfers changes in the Kernel tables between cluster members

Answer: A

NEW QUESTION 9

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	NBT	Drop	- None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https ssh	Accept	Log	Policy Targets
3	Stealth	* Any	GW-R7730	* 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	https http	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 10

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 10

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

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

Answer: B

Explanation:

Ref: https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_Ad

NEW QUESTION 11

When enabling tracking on a rule, what is the default option?

- A. Accounting Log
- B. Extended Log
- C. Log
- D. Detailed Log

Answer: C

NEW QUESTION 15

What are the types of Software Containers?

- A. Smart Console, Security Management, and Security Gateway
- B. Security Management, Security Gateway, and Endpoint Security
- C. Security Management, Log & Monitoring, and Security Policy
- D. Security Management, Standalone, and Security Gateway

Answer: B

NEW QUESTION 16

What is the purpose of the CPCA process?

- A. Monitoring the status of processes
- B. Sending and receiving logs
- C. Communication between GUI clients and the SmartCenter server
- D. Generating and modifying certificates

Answer: D

NEW QUESTION 20

Which tool allows you to monitor the top bandwidth on smart console?

- A. Logs & Monitoring
- B. Smart Event
- C. Gateways & Servers Tab
- D. SmartView Monitor

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 23

Fill in the blanks: Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.

- A. 675, 389
- B. 389, 636
- C. 636, 290
- D. 290, 675

Answer: B

Explanation:

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS.

NEW QUESTION 25

John is the administrator of a R80 Security Management server managing r R77.30 Check Point Security Gateway. John is currently updating the network objects and amending the rules using SmartConsole. To make John's changes available to other administrators, and to save the database before installing a policy, what must John do?

- A. Logout of the session
- B. File > Save
- C. Install database
- D. Publish the session

Answer: D

Explanation:

Installing and Publishing

It is important to understand the differences between publishing and installing. You must do this:

After you did this: Publish

Opened a session in SmartConsole and made changes.

The Publish operation sends all SmartConsole modifications to other administrators, and makes the changes you made in a private session public.

Install the database

Modified network objects, such as servers, users, services, or IPS profiles, but not the Rule Base. Updates are installed on management servers and log servers.

Install a policy Changed the Rule Base.

The Security Management Server installs the updated policy and the entire database on Security Gateways (even if you did not modify any network objects).

NEW QUESTION 28

Core Protections are installed as part of what Policy?

- A. Access Control Policy.
- B. Desktop Firewall Policy
- C. Mobile Access Policy.
- D. Threat Prevention Policy.

Answer: A

Explanation:

Core protections - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy. ThreatCloud

protections - Updated from the Check Point cloud, (see Updating IPS Protections). These protections are part of the Threat Prevention policy.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 32

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

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

Answer: A

NEW QUESTION 37

Which is NOT an encryption algorithm that can be used in an IPSEC Security Association (Phase 2)?

- A. AES-GCM-256
- B. AES-CBC-256
- C. AES-GCM-128

Answer: B

NEW QUESTION 41

John is using Management HA. Which Smartcenter should be connected to for making changes?

- A. secondary Smartcenter
- B. active Smartcenter
- C. connect virtual IP of Smartcenter HA
- D. primary Smartcenter

Answer: B

NEW QUESTION 45

What are the advantages of a “shared policy” in R80?

- A. Allows the administrator to share a policy between all the users identified by the Security Gateway
- B. Allows the administrator to share a policy between all the administrators managing the Security Management Server
- C. Allows the administrator to share a policy so that it is available to use in another Policy Package
- D. Allows the administrator to install a policy on one Security Gateway and it gets installed on another managed Security Gateway

Answer: C

Explanation:

Ref: https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 46

Fill in the blank: _____ is the Gaia command that turns the server off.

- A. sysdown
- B. exit
- C. halt
- D. shut-down

Answer: C

NEW QUESTION 51

Fill in the blank: Service blades must be attached to a _____.

- A. Security Gateway
- B. Management container
- C. Management server
- D. Security Gateway container

Answer: A

NEW QUESTION 53

What licensing feature is used to verify licenses and activate new licenses added to the License and Contracts repository?

- A. Verification tool
- B. Verification licensing
- C. Automatic licensing
- D. Automatic licensing and Verification tool

Answer: D

NEW QUESTION 55

Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 56

In R80 Management, apart from using SmartConsole, objects or rules can also be modified using:

- A. 3rd Party integration of CLI and API for Gateways prior to R80.
- B. A complete CLI and API interface using SSH and custom CPCODE integration.
- C. 3rd Party integration of CLI and API for Management prior to R80.

D. A complete CLI and API interface for Management with 3rd Party integration.

Answer: B

NEW QUESTION 57

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 58

The Gateway Status view in SmartConsole shows the overall status of Security Gateways and Software Blades. What does the Status Attention mean?

- A. Cannot reach the Security Gateway.
- B. The gateway and all its Software Blades are working properly.
- C. At least one Software Blade has a minor issue, but the gateway works.
- D. Cannot make SIC between the Security Management Server and the Security Gateway

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 61

Gaia has two default user accounts that cannot be deleted. What are those user accounts?

- A. Admin and Default
- B. Expert and Clish
- C. Control and Monitor
- D. Admin and Monitor

Answer: D

NEW QUESTION 65

In order to see real-time and historical graph views of Security Gateway statistics in SmartView Monitor, what feature needs to be enabled on the Security Gateway?

- A. Logging & Monitoring
- B. None - the data is available by default
- C. Monitoring Blade
- D. SNMP

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

NEW QUESTION 69

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 71

What is the default tracking option of a rule?

- A. Tracking
- B. Log
- C. None
- D. Alert

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 73

A network administrator has informed you that they have identified a malicious host on the network, and instructed you to block it. Corporate policy dictates that firewall policy changes cannot be made at this time. What tool can you use to block this traffic?

- A. Anti-Bot protection
- B. Anti-Malware protection
- C. Policy-based routing
- D. Suspicious Activity Monitoring (SAM) rules

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 75

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 77

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 79

Which backup 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 82

Which SmartConsole application shows correlated logs and aggregated data to provide an overview of potential threats and attack patterns?

- A. SmartEvent
- B. SmartView Tracker
- C. SmartLog
- D. SmartView Monitor

Answer: A

Explanation:

<https://www.checkpoint.com/downloads/products/smartevent-datasheet.pdf>

NEW QUESTION 87

What type of NAT is a one-to-one relationship where each host is translated to a unique address?

- A. Source
- B. Static
- C. Hide
- D. Destination

Answer: B

NEW QUESTION 90

Which Check Point software blade provides Application Security and identity control?

- A. Identity Awareness
- B. Data Loss Prevention
- C. URL Filtering
- D. Application Control

Answer: D

Explanation:

Check Point Application Control provides the industry's strongest application security and identity control to organizations of all sizes.

NEW QUESTION 91

What Identity Agent allows packet tagging and computer authentication?

- A. Endpoint Security Client
- B. Full Agent
- C. Light Agent
- D. System Agent

Answer: B

Explanation:

Identity Agent Description Full

Default Identity AgentClosed that includes packet tagging and computer authentication. It applies to all users on the computer on which it is installed.

Administrator permissions are required to use the Full Identity Agent type. For the Full Identity Agent, you can enforce IP spoofing protection. In addition, you can leverage computer authentication if you specify computers in Access Roles.

Light

Default Identity Agent that does not include packet tagging and computer authentication. You can install this Identity Agent individually for each user on the target computer. Light Identity Agent type does not require Administrator permissions.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 94

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 99

What is the purpose of Captive Portal?

- A. It manages user permission in SmartConsole
- B. It provides remote access to SmartConsole
- C. It authenticates users, allowing them access to the Internet and corporate resources
- D. It authenticates users, allowing them access to the Gaia OS

Answer: C

Explanation:

Captive Portal is a simple method that authenticates users with a web interface. When users try to access a protected web resource, they enter authentication information in a form that shows in their web browser.

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_IdentityAwareness_AdminG

NEW QUESTION 104

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 109

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 110

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 114

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 115

In which scenario is it a valid option to transfer a license from one hardware device to another?

- A. From a 4400 Appliance to a 2200 Appliance
- B. From a 4400 Appliance to an HP Open Server
- C. From an IBM Open Server to an HP Open Server
- D. From an IBM Open Server to a 2200 Appliance

Answer: A

Explanation:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 116

Fill in the blank: The position of an implied rule is manipulated in the _____ window.

- A. NAT
- B. Firewall
- C. Global Properties
- D. Object Explorer

Answer: C

Explanation:

"Note - In addition, users can access the Implied Rules configurations through Global Properties and use the implied policy view below Configuration."

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 120

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: D

NEW QUESTION 122

Which option will match a connection regardless of its association with a VPN community?

- A. All Site-to-Site VPN Communities
- B. Accept all encrypted traffic
- C. All Connections (Clear or Encrypted)
- D. Specific VPN Communities

Answer: B

NEW QUESTION 123

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsible, which of these steps should NOT be performed:

- A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
- B. Change the Standby Security Management Server to Active.
- C. Change the Active Security Management Server to Standby.
- D. Manually synchronize the Active and Standby Security Management Servers.

Answer: A

NEW QUESTION 124

Choose what BEST describes users on Gaia Platform.

- A. There are two default users and neither can be deleted.
- B. There are two default users and one cannot be deleted.
- C. There is one default user that can be deleted.
- D. There is one default user that cannot be deleted.

Answer: A

Explanation:

These users are created by default and cannot be deleted: admin

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

monitor

Has read-only capabilities for all features in the Gaia Portal and the Gaia Clish, and can change its own password.

You must give a password for this user before the account can be used.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/U

NEW QUESTION 128

Using R80 Smart Console, what does a “pencil icon” in a rule mean?

- A. I have changed this rule
- B. Someone else has changed this rule
- C. This rule is managed by check point's SOC
- D. This rule can't be changed as it's an implied rule

Answer: A

NEW QUESTION 129

The “Hit count” feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits even if the Track option is set to “None”?

- A. No, it will not work independentl
- B. Hit Count will be shown only for rules with Track options set as Log or alert
- C. Yes, it will work independently as long as “analyze all rules” tick box is enabled on the Security Gateway
- D. No, it will not work independently because hit count requires all rules to be logged
- E. Yes, it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways

Answer: D

NEW QUESTION 131

Which back up method uses the command line to create an image of the OS?

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

Answer: D

NEW QUESTION 134

Which of the following is considered a "Subscription Blade", requiring renewal every 1-3 years?

- A. IPS blade
- B. IPSEC VPN Blade
- C. Identity Awareness Blade
- D. Firewall Blade

Answer: A

NEW QUESTION 138

Fill in the blank: When a policy package is installed, _____ are also distributed to the target installation Security Gateways.

- A. User and objects databases
- B. Network databases
- C. SmartConsole databases
- D. User databases

Answer: A

Explanation:

A policy package is a collection of different types of policies. After installation, the Security Gateway enforces all the policies in the package. A policy package can have one or more of these policy types:

The installation process:

If there are verification errors, the policy is not installed. If there are verification warnings (for example, if anti-spoofing is not enabled for a Security Gateway with multiple interfaces), the policy package is installed with a warning.

NEW QUESTION 143

Which of these is NOT a feature or benefit of Application Control?

- A. Eliminate unknown and unwanted applications in your network to reduce IT complexity and application risk.
- B. Identify and control which applications are in your IT environment and which to add to the IT environment.
- C. Scans the content of files being downloaded by users in order to make policy decisions.
- D. Automatically identify trusted software that has authorization to run

Answer: C

Explanation:

File scanning is a job for ThreatCloud and it sandboxes/scrubs files.

NEW QUESTION 147

What is the most complete definition of the difference between the Install Policy button on the SmartConsole's tab, and the Install Policy within a specific policy?

- A. The Global one also saves and published the session before installation.
- B. The Global one can install multiple selected policies at the same time.
- C. The local one does not install the Anti-Malware policy along with the Network policy.
- D. The second one pre-select the installation for only the current policy and for the applicable gateways.

Answer: D

NEW QUESTION 152

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

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

Answer: A

NEW QUESTION 155

What is the purpose of a Stealth Rule?

- A. A rule used to hide a server's IP address from the outside world.
- B. A rule that allows administrators to access SmartDashboard from any device.
- C. To drop any traffic destined for the firewall that is not otherwise explicitly allowed.
- D. A rule at the end of your policy to drop any traffic that is not explicitly allowed.

Answer: C

NEW QUESTION 157

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 162

Fill in the blank: Each cluster, at a minimum, should have at least _____ interfaces.

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

Answer: C

NEW QUESTION 163

Application Control/URL filtering database library is known as:

- A. Application database
- B. AppWiki
- C. Application-Forensic Database
- D. Application Library

Answer: B

Explanation:

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 166

Which one of the following is a way that the objects can be manipulated using the new API integration in R80 Management?

- A. Microsoft Publisher
- B. JSON
- C. Microsoft Word
- D. RC4 Encryption

Answer: B

NEW QUESTION 167

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

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

Answer: A

NEW QUESTION 172

Fill in the blank: An LDAP server holds one or more _____.

- A. Server Units
- B. Administrator Units
- C. Account Units
- D. Account Servers

Answer: C

NEW QUESTION 176

Which of the following commands is used to monitor cluster members?

- A. cphaprob state
- B. cphaprob status
- C. cphaprob
- D. cluster state

Answer: A

NEW QUESTION 181

Which of the following is used to enforce changes made to a Rule Base?

- A. Publish database
- B. Save changes
- C. Install policy
- D. Activate policy

Answer: A

NEW QUESTION 185

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

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

Answer: D

Explanation:

You can change the User Directory templates. Users associated with this template get the changes immediately. If you change user definitions manually in SmartConsole, the changes are immediate on the server.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 186

What are the three components for Check Point Capsule?

- A. Capsule Docs, Capsule Cloud, Capsule Connect
- B. Capsule Workspace, Capsule Cloud, Capsule Connect
- C. Capsule Workspace, Capsule Docs, Capsule Connect
- D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 188

Where can administrator edit a list of trusted SmartConsole clients?

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

Answer: B

NEW QUESTION 193

Why is a Central License the preferred and recommended method of licensing?

- A. Central Licensing is actually not supported with Gaia.
- B. Central Licensing is the only option when deploying Gaia
- C. Central Licensing ties to the IP address of a gateway and can be changed to any gateway if needed.
- D. Central Licensing ties to the IP address of the management server and is not dependent on the IP of any gateway in the event it changes.

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To

NEW QUESTION 196

Which of the following commands is used to monitor cluster members in CLI?

- A. show cluster state
- B. show active cluster
- C. show clusters
- D. show running cluster

Answer: A

NEW QUESTION 201

Which tool is used to enable ClusterXL?

- A. SmartUpdate
- B. cpconfig
- C. SmartConsole
- D. sysconfig

Answer: B

NEW QUESTION 204

When should you generate new licenses?

- A. Before installing contract files.
- B. After a device upgrade.
- C. When the existing license expires, license is upgraded or the IP-address associated with the license changes.
- D. Only when the license is upgraded.

Answer: C

NEW QUESTION 208

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

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

Answer: A

NEW QUESTION 212

Which two of these Check Point Protocols are used by ?

- A. ELA and CPD
- B. FWD and LEA
- C. FWD and CPLOG
- D. ELA and CPLOG

Answer: B

NEW QUESTION 215

After the initial installation on Check Point appliance, you notice that the Management interface and default gateway are incorrect. Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

- A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
- B. add interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0.0.0.0.0 gw 192.168.80.1 onsave config
- D. add interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Answer: A

NEW QUESTION 217

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

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

Answer: C

Explanation:

application firewalls, or application layer firewalls, use a series of configured policies to determine whether to block or allow communications to or from an app.

NEW QUESTION 221

Which of the following is used to initially create trust between a Gateway and Security Management Server?

- A. Internal Certificate Authority
- B. Token
- C. One-time Password
- D. Certificate

Answer: C

Explanation:

To establish the initial trust, a gateway and a Security Management Server use a one-time password. After the initial trust is established, further communication is based on security certificates.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 222

You are going to perform a major upgrade. Which back up solution should you use to ensure your database can be restored on that device?

- A. backup
- B. logswitch
- C. Database Revision
- D. snapshot

Answer: D

Explanation:

The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system. Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported.

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

NEW QUESTION 226

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

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

Answer: A

NEW QUESTION 227

Which icon in the WebUI indicates that read/write access is enabled?

- A. Pencil
- B. Padlock
- C. Book
- D. Eyeglasses

Answer: A

NEW QUESTION 228

An administrator can use section titles to more easily navigate between large rule bases. Which of these statements is FALSE?

- A. Section titles are not sent to the gateway side.
- B. These sections are simple visual divisions of the Rule Base and do not hinder the order of rule enforcement.
- C. A Sectional Title can be used to disable multiple rules by disabling only the sectional title.
- D. Sectional Titles do not need to be created in the SmartConsole.

Answer: C

Explanation:

Section titles are only for visual categorization of rules.

NEW QUESTION 231

Which key is created during Phase 2 of a site-to-site VPN?

- A. Pre-shared secret
- B. Diffie-Hellman Public Key
- C. Symmetrical IPSec key
- D. Diffie-Hellman Private Key

Answer: C

NEW QUESTION 232

To quickly review when Threat Prevention signatures were last updated, which Threat Tool would an administrator use?

- A. Protections
- B. IPS Protections
- C. Profiles
- D. ThreatWiki

Answer: B

NEW QUESTION 234

Which type of attack can a firewall NOT prevent?

- A. Network Bandwidth Saturation
- B. Buffer Overflow
- C. SYN Flood
- D. SQL Injection

Answer: A

NEW QUESTION 237

Is it possible to have more than one administrator connected to a Security Management Server at once?

- A. Yes, but only if all connected administrators connect with read-only permissions.
- B. Yes, but objects edited by one administrator will be locked for editing by others until the session is published.
- C. No, only one administrator at a time can connect to a Security Management Server
- D. Yes, but only one of those administrators will have write-permission
- E. All others will have read-only permission.

Answer: B

NEW QUESTION 238

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 240

Check Point ClusterXL Active/Active deployment is used when:

- A. Only when there is Multicast solution set up
- B. There is Load Sharing solution set up
- C. Only when there is Unicast solution set up
- D. There is High Availability solution set up

Answer: D

NEW QUESTION 241

DLP and Geo Policy are examples of what type of Policy?

- A. Inspection Policies

- B. Shared Policies
- C. Unified Policies
- D. Standard Policies

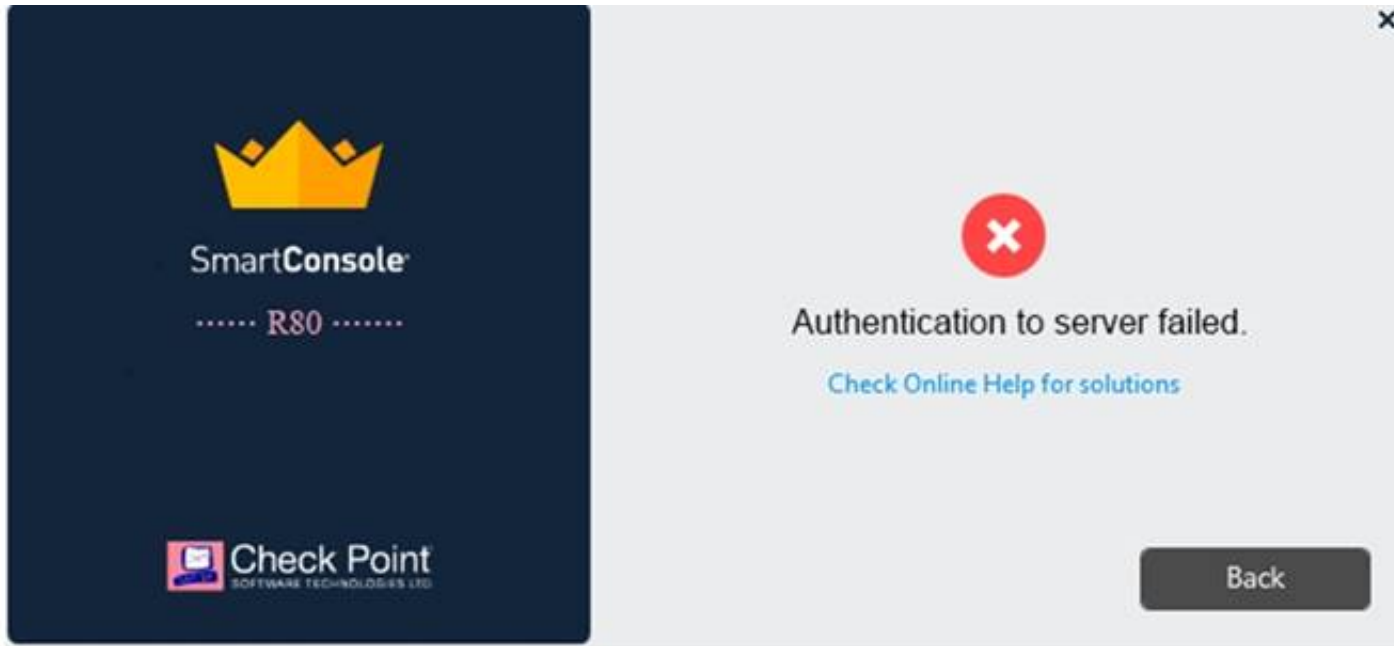
Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_NextGenSecurityGateway_G

NEW QUESTION 246

Vanessa is attempting to log into the Gaia Web Portal. She is able to login successfully. Then she tries the same username and password for SmartConsole but gets the message in the screenshot image below. She has checked that the IP address of the Server is correct and the username and password she used to login into Gaia is also correct.



What is the most likely reason?

- A. Check Point R80 SmartConsole authentication is more secure than in previous versions and Vanessa requires a special authentication key for R80 SmartConsole
- B. Check that the correct key details are used.
- C. Check Point Management software authentication details are not automatically the same as the Operating System authentication detail
- D. Check that she is using the correct details.
- E. SmartConsole Authentication is not allowed for Vanessa until a Super administrator has logged in first and cleared any other administrator sessions.
- F. Authentication failed because Vanessa's username is not allowed in the new Threat Prevention console update checks even though these checks passed with Gaia.

Answer: B

NEW QUESTION 251

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

- A. Remote Access
- B. Cloud IdP (Identity Provider)
- C. Active Directory Query
- D. RADIUS

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 252

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 254

A Check Point Software license consists of two components, the Software Blade and the Software Container. There are _____ types of Software Containers: _____.

- A. Two; Security Management and Endpoint Security
- B. Two; Endpoint Security and Security Gateway
- C. Three; Security Management, Security Gateway, and Endpoint Security
- D. Three; Security Gateway, Endpoint Security, and Gateway Management

Answer: C

Explanation:

There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security. Ref: <https://downloads.checkpoint.com/dc/download.htm?ID=11608>

NEW QUESTION 256

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

- A. INSPECT Engine
- B. Next-Generation Firewall
- C. Packet Filtering
- D. Application Layer Firewall

Answer: A

Explanation:

Check Point FireWall-1's Stateful Inspection overcomes the limitations of the previous two approaches by providing full application-layer awareness without breaking the client/server model. With Stateful Inspection, the packet is intercepted at the network layer, but then the INSPECT Engine takes over. It extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts. This provides a solution which is highly secure and offers maximum performance, scalability, and extensibility.

NEW QUESTION 259

Which of the following is NOT supported by Bridge Mode on the Check Point Security Gateway?

- A. Data Loss Prevention
- B. Antivirus
- C. Application Control
- D. NAT

Answer: D

Explanation:

NAT rules (specifically, Firewall kernel in logs shows the traffic as accepted, but Security Gateway does not actually forward it). For more information, see sk106146. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/T

NEW QUESTION 261

Identity Awareness allows easy configuration for network access and auditing based on what three items?

- A. Client machine IP address.
- B. Network location, the identity of a user and the identity of a machine.
- C. Log server IP address.
- D. Gateway proxy IP address.

Answer: B

NEW QUESTION 265

When using Automatic Hide NAT, what is enabled by default?

- A. Source Port Address Translation (PAT)
- B. Static NAT
- C. Static Route
- D. HTTPS Inspection

Answer: A

Explanation:

Hiding multiple IP addresses behind one, gateway, IP address requires PAT to differentiate between traffic.

NEW QUESTION 270

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

- A. ThreatWiki
- B. Whitelist Files
- C. AppWiki
- D. IPS Protections

Answer: A

NEW QUESTION 271

Which option in a firewall rule would only match and allow traffic to VPN gateways for one Community in common?

- A. All Connections (Clear or Encrypted)
- B. Accept all encrypted traffic
- C. Specific VPN Communities
- D. All Site-to-Site VPN Communities

Answer: C

NEW QUESTION 276

Which of the following licenses are considered temporary?

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

Answer: A

NEW QUESTION 281

What default layers are included when creating a new policy layer?

- A. Application Control, URL Filtering and Threat Prevention
- B. Access Control, Threat Prevention and HTTPS Inspection
- C. Firewall, Application Control and IPSec VPN
- D. Firewall, Application Control and IPS

Answer: B

NEW QUESTION 282

What object type would you use to grant network access to an LDAP user group?

- A. Access Role
- B. User Group
- C. SmartDirectory Group
- D. Group Template

Answer: B

NEW QUESTION 287

URL Filtering cannot be used to:

- A. Control Bandwidth issues
- B. Control Data Security
- C. Improve organizational security
- D. Decrease legal liability

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 290

Which two Identity Awareness commands are used to support identity sharing?

- A. Policy Decision Point (PDP) and Policy Enforcement Point (PEP)
- B. Policy Enforcement Point (PEP) and Policy Manipulation Point (PMP)
- C. Policy Manipulation Point (PMP) and Policy Activation Point (PAP)
- D. Policy Activation Point (PAP) and Policy Decision Point (PDP)

Answer: A

NEW QUESTION 292

How is communication between different Check Point components secured in R80? As with all questions, select the best answer.

- A. By using IPSEC
- B. By using SIC
- C. By using ICA
- D. By using 3DES

Answer: B

NEW QUESTION 296

Which default Gaia user has full read/write access?

- A. admin
- B. superuser
- C. monitor
- D. altuser

Answer: A

Explanation:

Has full read/write capabilities for all Gaia features, from the Gaia Portal and the Gaia Clish. This user has a User ID of 0, and therefore has all of the privileges of a root user. monitor Has read-only capabilities for all features in the Gaia Portal and the Gaia Clish, and can change its own password. You must give a password for this user before the account can be used.

NEW QUESTION 300

Which application is used for the central management and deployment of licenses and packages?

- A. SmartProvisioning
- B. SmartLicense
- C. SmartUpdate
- D. Deployment Agent

Answer: C

NEW QUESTION 301

Which option, when applied to a rule, allows all encrypted and non-VPN traffic that matches the rule?

- A. All Site-to-Site VPN Communities
- B. Accept all encrypted traffic
- C. All Connections (Clear or Encrypted)
- D. Specific VPN Communities

Answer: B

NEW QUESTION 306

Fill in the blank: It is Best Practice to have a _____ rule at the end of each policy layer.

- A. Explicit Drop
- B. Implied Drop
- C. Explicit CleanUp
- D. Implicit Drop

Answer: C

NEW QUESTION 309

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

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

Answer: B

NEW QUESTION 311

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 316

Which of the following cannot be configured in an Access Role Object?

- A. Networks
- B. Users
- C. Time
- D. Machines

Answer: C

Explanation:

Access Role objects includes one or more of these objects: Networks.

Users and user groups. Computers and computer groups. Remote Access Clients.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

NEW QUESTION 317

Security Gateway software blades must be attached to what?

- A. Security Gateway
- B. Security Gateway container

- C. Management server
- D. Management container

Answer: B

Explanation:

Security Management and Security Gateway Software Blades must be attached to a Software Container to be licensed.
<https://downloads.checkpoint.com/dc/download.htm?ID=11608>

NEW QUESTION 320

Fill in the blank: In order to install a license, it must first be added to the _____.

- A. User Center
- B. Package repository
- C. Download Center Web site
- D. License and Contract repository

Answer: B

NEW QUESTION 325

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

- A. Save Policy
- B. Install Database
- C. Save session
- D. Install Policy

Answer: D

NEW QUESTION 326

Which tool is used to enable cluster membership on a Gateway?

- A. SmartUpdate
- B. cpconfig
- C. SmartConsole
- D. sysconfig

Answer: B

Explanation:

References:

NEW QUESTION 331

Fill in the blank: Once a certificate is revoked from the Security GateWay by the Security Management Server, the certificate information is _____.

- A. Sent to the Internal Certificate Authority.
- B. Sent to the Security Administrator.
- C. Stored on the Security Management Server.
- D. Stored on the Certificate Revocation List.

Answer: D

NEW QUESTION 333

In which scenario will an administrator need to manually define Proxy ARP?

- A. When they configure an "Automatic Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
- B. When they configure an "Automatic Hide NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
- C. When they configure a "Manual Static NAT" which translates to an IP address that does not belong to one of the firewall's interfaces.
- D. When they configure a "Manual Hide NAT" which translates to an IP address that belongs to one of the firewall's interfaces.

Answer: C

NEW QUESTION 336

What protocol is specifically used for clustered environments?

- A. Clustered Protocol
- B. Synchronized Cluster Protocol
- C. Control Cluster Protocol
- D. Cluster Control Protocol

Answer: D

NEW QUESTION 339

Which of the following log queries would show only dropped packets with source address of 192.168.1.1 and destination address of 172.26.1.1?

- A. src:192.168.1.1 OR dst:172.26.1.1 AND action:Drop
- B. src:192.168.1.1 AND dst:172.26.1.1 AND action:Drop
- C. 192.168.1.1 AND 172.26.1.1 AND drop
- D. 192.168.1.1 OR 172.26.1.1 AND action:Drop

Answer: B

NEW QUESTION 344

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. You achieve compartmentalization by allowing a large number of users to be distributed across several servers
- C. Information on a user is hidden, yet distributed across several servers.
- D. You gain High Availability by replicating the same information on several servers

Answer: C

NEW QUESTION 347

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 349

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

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

Answer: D

NEW QUESTION 350

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

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

Answer: D

NEW QUESTION 351

How Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VP
- B. Capsule Workspace provides a Desktop with usable applications
- C. Capsule Workspace can provide access to any application
- D. Capsule Connect provides Business data isolation
- E. Capsule Connect does not require an installed application at client

Answer: A

NEW QUESTION 356

Log query results can be exported to what file format?

- A. Word Document (docx)
- B. Comma Separated Value (csv)
- C. Portable Document Format (pdf)
- D. Text (txt)

Answer: B

NEW QUESTION 359

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete
- B. Threat Extraction always delivers a file and takes less than a second to complete

- C. Threat Emulation never delivers a file that takes less than a second to complete
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Answer: B

NEW QUESTION 360

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

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

Answer: B

Explanation:

Shared Policies

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

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

Description Mobile Access

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

DLP

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

Geo Policy

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

NEW QUESTION 365

You have created a rule at the top of your Rule Base to permit Guest Wireless access to the Internet. However, when guest users attempt to reach the Internet, they are not seeing the splash page to accept your Terms of Service, and cannot access the Internet. How can you fix this?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

- A. Right click Accept in the rule, select “More”, and then check “Enable Identity Captive Portal”
- B. On the firewall object, Legacy Authentication screen, check “Enable Identity Captive Portal”
- C. In the Captive Portal screen of Global Properties, check “Enable Identity Captive Portal”
- D. On the Security Management Server object, check the box “Identity Logging”

Answer: A

NEW QUESTION 370

What is a role of Publishing?

- A. The Publish operation sends the modifications made via SmartConsole in the private session and makes them public
- B. The Security Management Server installs the updated policy and the entire database on Security Gateways
- C. The Security Management Server installs the updated session and the entire Rule Base on Security Gateways
- D. Modifies network objects, such as servers, users, services, or IPS profiles, but not the Rule Base

Answer: A

NEW QUESTION 375

Identity Awareness allows the Security Administrator to configure network access based on which of the following?

- A. Name of the application, identity of the user, and identity of the machine
- B. Identity of the machine, username, and certificate
- C. Network location, identity of a user, and identity of a machine
- D. Browser-Based Authentication, identity of a user, and network location

Answer: C

NEW QUESTION 376

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

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

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_QoS_AdminGuide/html_fram

NEW QUESTION 378

Which of the following is NOT a valid configuration screen of an Access Role Object?

- A. Users
- B. Networks
- C. Time
- D. Machines

Answer: C

NEW QUESTION 383

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

NEW QUESTION 385

What is the default shell of Gaia CLI?

- A. clish
- B. Monitor
- C. Read-only
- D. Bash

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Gaia_AdminGuide/Topics-GAG/C

NEW QUESTION 387

What is NOT an advantage of Stateful Inspection?

- A. High Performance
- B. Good Security
- C. No Screening above Network layer
- D. Transparency

Answer: A

NEW QUESTION 390

What Check Point tool is used to automatically update Check Point products for the Gaia OS?

- A. Check Point INSPECT Engine
- B. Check Point Upgrade Service Engine
- C. Check Point Update Engine
- D. Check Point Upgrade Installation Service

Answer: B

NEW QUESTION 392

Which of the following is NOT a policy type available for each policy package?

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

Answer: A

Explanation:

References:

NEW QUESTION 393

Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

- A. Application Control
- B. Threat Emulation
- C. Anti-Virus
- D. Advanced Networking Blade

Answer: B

NEW QUESTION 395

The CDT utility supports which of the following?

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

Answer: D

NEW QUESTION 399

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

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

Answer: D

NEW QUESTION 401

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

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

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 404

Name the authentication method that requires token authenticator.

- A. SecureID
- B. Radius
- C. DynamicID
- D. TACACS

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 407

What are the steps to configure the HTTPS Inspection Policy?

- A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
- B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
- C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
- D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: C

NEW QUESTION 409

What is UserCheck?

- A. Messaging tool user to verify a user's credentials
- B. Communication tool used to inform a user about a website or application they are trying to access
- C. Administrator tool used to monitor users on their network
- D. Communication tool used to notify an administrator when a new user is created

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T

NEW QUESTION 414

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-215.81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-215.81 Product From:

<https://www.2passeasy.com/dumps/156-215.81/>

Money Back Guarantee

156-215.81 Practice Exam Features:

- * 156-215.81 Questions and Answers Updated Frequently
- * 156-215.81 Practice Questions Verified by Expert Senior Certified Staff
- * 156-215.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-215.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year