

CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81



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

With URL Filtering, what portion of the traffic is sent to the Check Point Online Web Service for analysis?

- A. The complete communication is sent for inspection.
- B. The IP address of the source machine.
- C. The end user credentials.
- D. The host portion of the URL.

Answer: D

Explanation:

"A local cache that gives answers to 99% of URL categorization requests. When the cache does not have an answer, only the host name is sent to the Check Point Online Web Service for categorization. " https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/24853/FILE/CP_R77_ApplicationControlURL

NEW QUESTION 3

In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

- A. Limit
- B. Resource
- C. Custom Application / Site
- D. Network Object

Answer: B

NEW QUESTION 4

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 5

Fill in the blanks: Gaia can be configured using _____ the _____.

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

Answer: A

Explanation:

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

NEW QUESTION 6

Under which file is the proxy arp configuration stored?

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

Answer: D

NEW QUESTION 7

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

- A. Common Name
- B. Country
- C. User container
- D. Organizational Unit

Answer: C

NEW QUESTION 8

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

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

Answer: C

NEW QUESTION 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	nisp 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 10

Fill in the blank: The _____ feature allows administrators to share a policy with other policy packages.

- A. Concurrent policy packages
- B. Concurrent policies
- C. Global Policies
- D. Shared policies

Answer: D

Explanation:

"The Shared Policies section in the Security Policies shows the policies that are not in a Policy package. They are shared between all Policy packages."
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide

NEW QUESTION 10

URL Filtering employs a technology, which educates users on web usage policy in real time. What is the name of that technology?

- A. WebCheck
- B. UserCheck
- C. Harmony Endpoint
- D. URL categorization

Answer: B

Explanation:

UserCheck alerts users while attempting to browse a suspicious/blocked or otherwise policy-limited website through a message in their web browsers shown before the actual page loads.

NEW QUESTION 12

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 14

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 18

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

Which path below is available only when CoreXL is enabled?

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

Answer: C

NEW QUESTION 26

What is the purpose of the Clean-up Rule?

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

Answer: A

Explanation:

These are basic access control rules we recommend for all Rule Bases:

There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

NEW QUESTION 28

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 31

Which option would allow you to make a backup copy of the OS and Check Point configuration, without stopping Check Point processes?

- A. All options stop Check Point processes
- B. backup
- C. migrate export
- D. snapshot

Answer: D

NEW QUESTION 34

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: D

NEW QUESTION 39

Which Threat Prevention Software Blade provides protection from malicious software that can infect your network computers? (Choose the best answer.)

- A. IPS
- B. Anti-Virus
- C. Anti-Malware
- D. Content Awareness

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To "Check Point Antivirus Software Blade prevents and stops threats such as malware, viruses, and Trojans from entering and infecting a network"
Also here -<https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf>

NEW QUESTION 42

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 44

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 48

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 54

Session unique identifiers are passed to the web api using which http header option?

- A. X-chkp-sid
- B. Accept-Charset
- C. Proxy-Authorization
- D. Application

Answer: C

NEW QUESTION 57

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 61

Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 62

How do logs change when the "Accounting" tracking option is enabled on a traffic rule?

- A. Involved traffic logs will be forwarded to a log server.
- B. Provides log details view email to the Administrator.
- C. Involved traffic logs are updated every 10 minutes to show how much data has passed on the connection.
- D. Provides additional information to the connected user.

Answer: C

Explanation:

Accounting - Select this to update the log at 10 minutes intervals, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time. https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGu

NEW QUESTION 67

Fill in the blanks: The _____ collects logs and sends them to the _____.

- A. Log server; Security Gateway
- B. Log server; security management server
- C. Security management server; Security Gateway
- D. Security Gateways; log server

Answer: D

Explanation:

Gateways send their logs to the log server.

NEW QUESTION 70

What is the SOLR database for?

- A. Used for full text search and enables powerful matching capabilities
- B. Writes data to the database and full text search
- C. Serves GUI responsible to transfer request to the DLE server
- D. Enables powerful matching capabilities and writes data to the database

Answer: A

NEW QUESTION 73

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 74

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 75

You have successfully backed up your Check Point configurations without the OS information. What command would you use to restore this backup?

- A. restore_backup
- B. import backup
- C. cp_merge
- D. migrate import

Answer: A

NEW QUESTION 77

Fill in the blank: Back up and restores can be accomplished through _____.

- A. SmartConsole, WebUI, or CLI
- B. WebUI, CLI, or SmartUpdate
- C. CLI, SmartUpdate, or SmartBackup
- D. SmartUpdate, SmartBackup, or SmartConsole

Answer: A

Explanation:

Backup and Restore These options let you: To back up a configuration:
The Backup window opens.

NEW QUESTION 78

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 82

In HTTPS Inspection policy, what actions are available in the "Actions" column of a rule?

- A. "Inspect", "Bypass"
- B. "Inspect", "Bypass", "Categorize"
- C. "Inspect", "Bypass", "Block"
- D. "Detect", "Bypass"

Answer: A

Explanation:

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

NEW QUESTION 85

Which deployment adds a Security Gateway to an existing environment without changing IP routing?

- A. Distributed
- B. Bridge Mode
- C. Remote
- D. Standalone

Answer: B

NEW QUESTION 89

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 90

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 94

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 99

What is the default shell for the command line interface?

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

Answer: A

Explanation:

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

NEW QUESTION 104

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 105

View the rule below. What does the pen-symbol in the left column mean?

3	 HR can access to social network applications	 HR	 Internet
4	 All employees can access YouTube for work purposes	 Corporate LANs  Branch Office LAN  Data Center LAN	 Internet

- A. Those rules have been published in the current session.
- B. Rules have been edited by the logged in administrator, but the policy has not been published yet.
- C. Another user has currently locked the rules for editing.
- D. The configuration lock is present
- E. Click the pen symbol in order to gain the lock.

Answer: B

NEW QUESTION 106

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 109

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

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

Answer: B

NEW QUESTION 114

Your internal networks 10.1.1.0/24, 10.2.2.0/24 and 192.168.0.0/16 are behind the Internet Security Gateway. Considering that Layer 2 and Layer 3 setup is correct, what are the steps you will need to do in SmartConsole in order to get the connection working?

- A. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway's external IP.3. Publish and install the policy.
- B. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish the policy.
- C. 1. Define an accept rule in Security Policy.2. Define automatic NAT for each network to NAT the networks behind a public IP.3. Publish and install the policy.
- D. 1. Define an accept rule in Security Policy.2. Define Security Gateway to hide all internal networks behind the gateway's external IP.3. Publish the policy.

Answer: C

NEW QUESTION 119

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 122

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 123

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 124

What is true about the IPS-Blade?

- A. in R80, IPS is managed by the Threat Prevention Policy
- B. in R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
- C. in R80, IPS Exceptions cannot be attached to "all rules"
- D. in R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 125

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 126

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 128

R80 is supported by which of the following operating systems:

- A. Windows only
- B. Gaia only
- C. Gaia, SecurePlatform, and Windows
- D. SecurePlatform only

Answer: B

NEW QUESTION 131

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 136

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 137

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 141

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 145

In _____ NAT, the _____ is translated.

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

Answer: A

NEW QUESTION 148

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 151

You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?

- A. Open SmartLog and connect remotely to the IP of the wireless controller
- B. Open SmartView Tracker and filter the logs for the IP address of the tablet
- C. Open SmartView Tracker and check all the IP logs for the tablet
- D. Open SmartLog and query for the IP address of the Manager's tablet

Answer: B

NEW QUESTION 152

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 157

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 161

Which Threat Prevention Profile is not included by default in R80 Management?

- A. Basic – Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance
- B. Optimized – Provides excellent protection for common network products and protocols against recent or popular attacks
- C. Strict – Provides a wide coverage for all products and protocols, with impact on network performance
- D. Recommended – Provides all protection for all common network products and servers, with impact on network performance

Answer: D

NEW QUESTION 162

Which part of SmartConsole allows administrators to add, edit delete, and clone objects?

- A. Object Browser
- B. Object Editor

- C. Object Navigator
- D. Object Explorer

Answer: D

NEW QUESTION 164

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 165

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 167

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 171

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 175

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 178

Which configuration element determines which traffic should be encrypted into a VPN tunnel vs. sent in the clear?

- A. The firewall topologies
- B. NAT Rules
- C. The Rule Base
- D. The VPN Domains

Answer: C

NEW QUESTION 180

R80.10 management server can manage gateways with which versions installed?

- A. Versions R77 and higher
- B. Versions R76 and higher
- C. Versions R75.20 and higher
- D. Version R75 and higher

Answer: B

NEW QUESTION 185

What needs to be configured if the NAT property 'Translate destination on client side' is not enabled in Global properties?

- A. A host route to route to the destination IP
- B. Use the file local.arp to add the ARP entries for NAT to work
- C. Nothing, the Gateway takes care of all details necessary
- D. Enabling 'Allow bi-directional NAT' for NAT to work correctly

Answer: C

NEW QUESTION 186

One of major features in R80.x SmartConsole is concurrent administration. Which of the following is NOT possible considering that AdminA, AdminB, and AdminC are editing the same Security Policy?

- A. AdminC sees a lock icon which indicates that the rule is locked for editing by another administrator.
- B. AdminA and AdminB are editing the same rule at the same time.
- C. AdminB sees a pencil icon next the rule that AdminB is currently editing.
- D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Answer: B

NEW QUESTION 190

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

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

Answer: D

NEW QUESTION 191

Which of the following is used to extract state related information from packets and store that information in state tables?

- A. STATE Engine
- B. TRACK Engine
- C. RECORD Engine
- D. INSPECT Engine

Answer: D

Explanation:

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.

NEW QUESTION 193

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 198

When dealing with rule base layers, what two layer types can be utilized?

- A. Ordered Layers and Inline Layers
- B. Inbound Layers and Outbound Layers
- C. R81.10 does not support Layers
- D. Structured Layers and Overlap Layers

Answer: A

Explanation:

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

NEW QUESTION 201

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 203

To ensure that VMAC mode is enabled, which CLI command you should run on all cluster members? Choose the best answer.

- A. fw ctl set int fwha vmac global param enabled
- B. fw ctl get int fwha vmac global param enabled; result of command should return value 1
- C. cphaprob -a if
- D. fw ctl get int fwha_vmac_global_param_enabled; result of command should return value 1

Answer: B

NEW QUESTION 207

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 211

When configuring Spoof Tracking, which tracking actions can an administrator select to be done when spoofed packets are detected?

- A. Log, send snmp trap, email
- B. Drop packet, alert, none
- C. Log, alert, none
- D. Log, allow packets, email

Answer: C

Explanation:

Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected:

NEW QUESTION 214

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 215

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 216

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

- A. The amount of logs being stored is less than previous versions.
- B. New Smart-1 appliances double the physical memory install.
- C. Indexing Engine indexes logs for faster search results.

D. SmartConsole now queries results directly from the Security Gateway.

Answer: B

NEW QUESTION 218

Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 221

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

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

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. Ref: <https://www.checkpoint.com/products/smartevent/>

NEW QUESTION 226

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 228

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 231

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 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 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 234

When comparing Stateful Inspection and Packet Filtering, what is a benefit that Stateful Inspection offers over Packet Filtering?

- A. Stateful Inspection offers unlimited connections because of virtual memory usage.
- B. Stateful Inspection offers no benefits over Packet Filtering.
- C. Stateful Inspection does not use memory to record the protocol used by the connection.
- D. Only one rule is required for each connection.

Answer: D

NEW QUESTION 237

Which of the following is NOT a valid deployment option for R80?

- A. All-in-one (stand-alone)

- B. Log server
- C. SmartEvent
- D. Multi-domain management server

Answer: D

NEW QUESTION 242

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

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

Answer: A

NEW QUESTION 246

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

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

Answer: A

Explanation:

There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security.

NEW QUESTION 250

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 252

When an Admin logs into SmartConsole and sees a lock icon on a gateway object and cannot edit that object, what does that indicate?

- A. The gateway is not powered on.
- B. Incorrect routing to reach the gateway.
- C. The Admin would need to login to Read-Only mode
- D. Another Admin has made an edit to that object and has yet to publish the change.

Answer: D

NEW QUESTION 254

True or False: The destination server for Security Gateway logs depends on a Security Management Server configuration.

- A. False, log servers are configured on the Log Server General Properties
- B. True, all Security Gateways will only forward logs with a SmartCenter Server configuration
- C. True, all Security Gateways forward logs automatically to the Security Management Server
- D. False, log servers are enabled on the Security Gateway General Properties

Answer: B

NEW QUESTION 258

The competition between stateful inspection and proxies was based on performance, protocol support, and security. Considering stateful Inspections and Proxies, which statement is correct?

- A. Stateful Inspection is limited to Layer 3 visibility, with no Layer 4 to Layer 7 visibility capabilities.
- B. When it comes to performance, proxies were significantly faster than stateful inspection firewalls.
- C. Proxies offer far more security because of being able to give visibility of the payload (the data).
- D. When it comes to performance, stateful inspection was significantly faster than proxies.

Answer: C

NEW QUESTION 263

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 267

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 272

Which tool allows for the automatic updating of the Gaia OS and Check Point products installed on the Gaia OS?

- A. CPASE - Check Point Automatic Service Engine
- B. CPAUE - Check Point Automatic Update Engine
- C. CPDAS - Check Point Deployment Agent Service
- D. CPUSE - Check Point Upgrade Service Engine

Answer: D

Explanation:

Check Point Update Service Engine (CPUSE), also known as Deployment Agent [DA], is an advanced and intuitive mechanism for software deployment on Gaia OS, which supports deployments of single HotFixes (HF), of HotFix Accumulators (Jumbo), and of Major Versions.
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=

NEW QUESTION 276

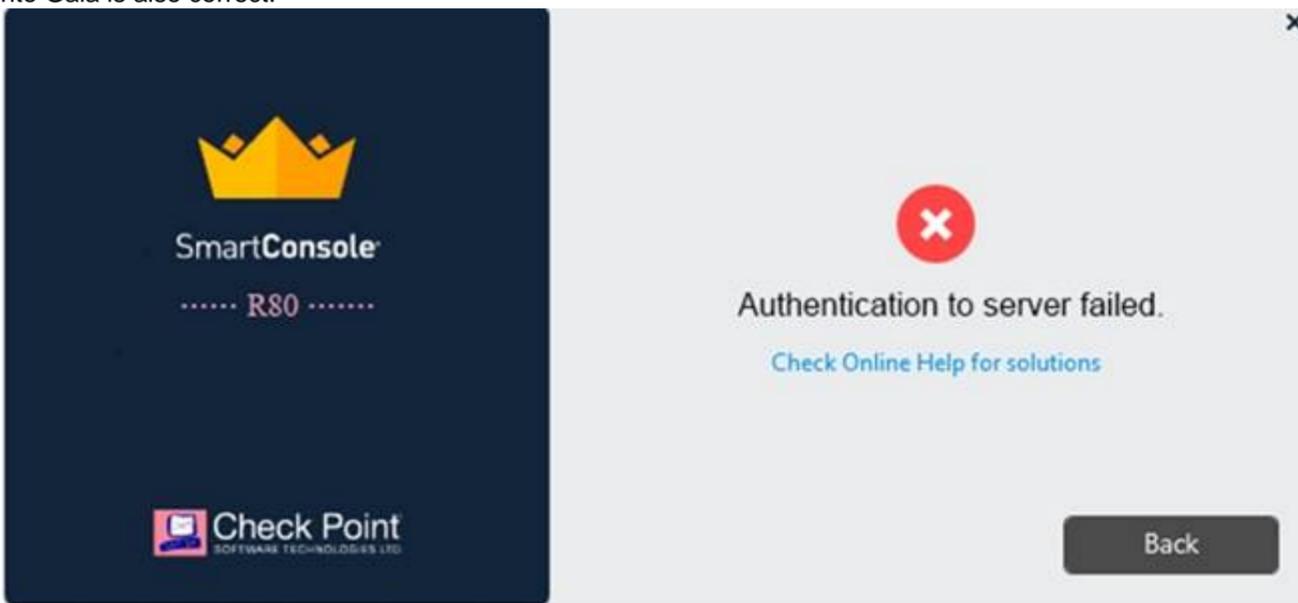
When changes are made to a Rule base, it is important to _____ to enforce changes.

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

Answer: C

NEW QUESTION 278

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 281

A security zone is a group of one or more network interfaces from different centrally managed gateways. What is considered part of the zone?

- A. The zone is based on the network topology and determined according to where the interface leads to.
- B. Security Zones are not supported by Check Point firewalls.
- C. The firewall rule can be configured to include one or more subnets in a zone.
- D. The local directly connected subnet defined by the subnet IP and subnet mask.

Answer: A

Explanation:

The Interface window opens. The Topology area of the General pane shows the Security Zone to which the interface is already bound. By default, the Security Zone is calculated according to where the interface Leads To.

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

NEW QUESTION 282

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 286

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 287

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 292

Which GUI tool can be used to view and apply Check Point licenses?

- A. cpconfig
- B. Management Command Line
- C. SmartConsole
- D. SmartUpdate

Answer: D

Explanation:

SmartUpdate GUI is the recommended way of managing licenses.

NEW QUESTION 294

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 296

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

- A. Distributed
- B. Standalone
- C. Bridge Mode
- D. Targeted

Answer: A

NEW QUESTION 297

Name the pre-defined Roles included in Gaia OS.

- A. AdminRole, and MonitorRole
- B. ReadWriteRole, and ReadyOnly Role
- C. AdminRole, cloningAdminRole, and Monitor Role
- D. AdminRole

Answer: A

NEW QUESTION 299

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 304

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 306

Fill in the blank: When tunnel test packets no longer invoke a response, SmartView Monitor displays _____ for the given VPN tunnel.

- A. Down
- B. No Response
- C. Inactive
- D. Failed

Answer: A

NEW QUESTION 308

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 310

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the "mgmt_cli" command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia's secure shell (clash)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 313

To enforce the Security Policy correctly, a Security Gateway requires:

- A. a routing table
- B. awareness of the network topology
- C. a Demilitarized Zone
- D. a Security Policy install

Answer: B

Explanation:

The network topology represents the internal network (both the LAN and the DMZ) protected by the gateway. The gateway must be aware of the layout of the network topology to:

NEW QUESTION 317

When should you generate new licenses?

- A. Before installing contract files.
- B. After an RMA procedure when the MAC address or serial number of the appliance changes.
- C. When the existing license expires, license is upgraded or the IP-address where the license is tied changes.
- D. Only when the license is upgraded.

Answer: C

NEW QUESTION 320

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 324

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: C

NEW QUESTION 328

Which of the following is NOT a role of the SmartCenter:

- A. Status monitoring
- B. Policy configuration
- C. Certificate authority
- D. Address translation

Answer: C

NEW QUESTION 329

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 (SMS). While configuring the VPN community to specify the pre-shared secret, the administrator did not find a box to input the pre-shared secret. Why does it not allow him to specify the pre-shared secret?

- A. The Gateway is an SMB device
- B. The checkbox “Use only Shared Secret for all external members” is not checked
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS
- D. Pre-shared secret is already configured in Global Properties

Answer: C

NEW QUESTION 332

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 335

Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 338

Fill in the blank: An identity server uses a _____ for user authentication.

- A. Shared secret
- B. Certificate
- C. One-time password
- D. Token

Answer: A

NEW QUESTION 339

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

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

Answer: C

Explanation:

Endpoint Identity Agents and Browser-Based Authentication - When a high level of security is necessary.

Captive Portal is used for distributing the Endpoint Identity Agent. IP Spoofing protection can be set to prevent packets from being IP spoofed.

NEW QUESTION 344

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 345

What is the most recommended installation method for Check Point appliances?

- A. SmartUpdate installation
- B. DVD media created with Check Point ISOMorphic
- C. USB media created with Check Point ISOMorphic
- D. Cloud based installation

Answer: C

NEW QUESTION 347

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 348

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 353

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 356

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 357

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

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

Answer: D

Explanation:

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

NEW QUESTION 360

How many users can have read/write access in Gaia Operating System at one time?

- A. One
- B. Three
- C. Two
- D. Infinite

Answer: A

Explanation:

if another user has r/w access, you need to use "lock database override" or "unlock database" to claim r/w access. Ref:
https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_Gaia_AdminGuide/html

NEW QUESTION 363

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 366

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

- A. Detects and blocks malware by correlating multiple detection engines before users are affected.
- B. Configure rules to limit the available network bandwidth for specified users or groups.
- C. Use UserCheck to help users understand that certain websites are against the company's security policy.
- D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A

NEW QUESTION 367

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 370

Most Check Point deployments use Gaia but which product deployment utilizes special Check Point code (with unification in R81.10)?

- A. Enterprise Network Security Appliances
- B. Rugged Appliances
- C. Scalable Platforms
- D. Small Business and Branch Office Appliances

Answer: A

NEW QUESTION 375

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. Anti-Virus

Answer: D

Explanation:

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

NEW QUESTION 376

Name the utility that is used to block activities that appear to be suspicious.

- A. Penalty Box
- B. Drop Rule in the rulebase
- C. Suspicious Activity Monitoring (SAM)
- D. Stealth rule

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_CLI_ReferenceGuide/Topics-CLIG

NEW QUESTION 379

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 384

What are the three main components of Check Point security management architecture?

- A. SmartConsole, Security Management, and Security Gateway
- B. Smart Console, Standalone, and Security Management
- C. SmartConsole, Security policy, and Logs & Monitoring
- D. GUI-Client, Security Management, and Security Gateway

Answer: A

NEW QUESTION 385

Which is a main component of the Check Point security management architecture?

- A. Identity Collector
- B. Endpoint VPN client
- C. SmartConsole
- D. Proxy Server

Answer: C

Explanation:

<https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/Part-1-The-Architecture/ba-p/88043> Security Gateway (SG) is usually deployed on the perimeter to control and secure traffic with Firewall and Threat Prevention capabilities.

Security Management Server (SMS) defines and controls security policies on the Gateways. It can also be used to as a log server with built-in system of log indexing (SmartLog) and event correlation (SmartEvent – a SIEM-like solution for Check Point products). Usually, SMS is the main element of central management

with multiple Security Gateways in operation. Nevertheless, you need an SMS even if your security system has a single gateway only. SmartConsole is a GUI administration tool to connect to SMS. Through this tool, a security administrator is able to prepare and apply security policies to the Security Gateways.

NEW QUESTION 389

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

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

Answer: C

NEW QUESTION 392

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 394

In SmartEvent, a correlation unit (CU) is used to do what?

- A. Collect security gateway logs, Index the logs and then compress the logs.
- B. Receive firewall and other software blade logs in a region and forward them to the primary log server.
- C. Analyze log entries and identify events.
- D. Send SAM block rules to the firewalls during a DOS attack.

Answer: C

Explanation:

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

NEW QUESTION 395

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 399

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

- A. Smart Cloud Services
- B. Load Sharing Mode Services
- C. Threat Agent Solution
- D. Public Cloud Services

Answer: A

NEW QUESTION 400

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 403

Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

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

Answer: B

Explanation:

The first rule is the automatic rule for the Accept All Encrypted Traffic feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.

* 2. Site to site VPN - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.

* 3. Remote access - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

NEW QUESTION 406

Which statement describes what Identity Sharing is in Identity Awareness?

- A. Management servers can acquire and share identities with Security Gateways
- B. Users can share identities with other users
- C. Security Gateways can acquire and share identities with other Security Gateways
- D. Administrators can share identities with other administrators

Answer: C

Explanation:

Identity Sharing

Best Practice - In environments that use many Security Gateways and AD Query, we recommend that you set only one Security Gateway to acquire identities from a given Active Directory domain controller for each physical site. If more than one Security Gateway gets identities from the same AD server, the AD server can become overloaded with WMI queries.

Set these options on the Identity Awareness > Identity Sharing page of the Security Gateway object:

NEW QUESTION 410

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 415

The purpose of the Communication Initialization process is to establish a trust between the Security Management Server and the Check Point gateways. Which statement best describes this Secure Internal Communication (SIC)?

- A. After successful initialization, the gateway can communicate with any Check Point node that possesses a SIC certificate signed by the same ICA.
- B. Secure Internal Communications authenticates the security gateway to the SMS before http communications are allowed.
- C. A SIC certificate is automatically generated on the gateway because the gateway hosts a subordinate CA to the SMS ICA.
- D. New firewalls can easily establish the trust by using the expert password defined on the SMS and the SMS IP address.

Answer: A

Explanation:

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

NEW QUESTION 419

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 421

How are the backups stored in Check Point appliances?

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

Answer: B

Explanation:

Backup configurations are stored in: /var/CPbackup/backups/

NEW QUESTION 426

What is the difference between SSL VPN and IPSec VPN?

- A. IPSec VPN does not require installation of a resident VPN client
- B. SSL VPN requires installation of a resident VPN client
- C. SSL VPN and IPSec VPN are the same
- D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser

Answer: D

NEW QUESTION 430

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 434

After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

- A. Security Gateway IP-address cannot be changed without re-establishing the trust
- B. The Security Gateway name cannot be changed in command line without re-establishing trust
- C. The Security Management Server name cannot be changed in SmartConsole without re-establishing trust
- D. The Security Management Server IP-address cannot be changed without re-establishing the trust

Answer: A

NEW QUESTION 438

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 439

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 444

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 448

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 451

You want to verify if there are unsaved changes in GAIa that will be lost with a reboot. What command can be used?

- A. show unsaved
- B. show save-state
- C. show configuration diff
- D. show config-state

Answer: D

NEW QUESTION 455

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 460

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 462

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

156-215.81 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 First Try
- * 156-215.81 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-215.81 Practice Test Here](#)