



CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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

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

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

Answer: C

NEW QUESTION 3

What is the best sync method in the ClusterXL deployment?

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

Answer: B

NEW QUESTION 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

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 6

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 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	http https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp	Accept	Log	Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	Policy Targets

What is the possible explanation for this?

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

Answer: B

NEW QUESTION 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 10

You are the Check Point administrator for Alpha Corp. You received a call that one of the users is unable to browse the Internet on their new tablet which is connected to the company wireless, which goes through a Check Point Gateway. How would you review the logs to see what is blocking this traffic?

- A. Open SmartLog and connect remotely to the wireless controller
- B. Open SmartEvent to see why they are being blocked
- C. Open SmartDashboard and review the logs tab
- D. From SmartConsole, go to the Log & Monitor and filter for the IP address of the tablet.

Answer: D

NEW QUESTION 15

Fill in the bank: In Office mode, a Security Gateway assigns a remote client to an IP address once _____ .

- A. the user connects and authenticates
- B. office mode is initiated
- C. the user requests a connection
- D. the user connects

Answer: A

Explanation:

Office Mode enables a Security Gateway to assign a remote client an IP address. The assignment takes place once the user connects and authenticates. The

assignment lease is renewed as long as the user is connected.

NEW QUESTION 17

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 18

A SAM rule is implemented to provide what function or benefit?

- A. Allow security audits.
- B. Handle traffic as defined in the policy.
- C. Monitor sequence activity.
- D. Block suspicious activity.

Answer: D

Explanation:

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

NEW QUESTION 20

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 22

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

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

Answer: B

NEW QUESTION 24

John is the administrator of a R80 Security Management server managing a 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 26

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"](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/To%20Check%20Point%20Antivirus%20Software%20Blade%20prevents%20and%20stops%20threats%20such%20as%20malware%2C%20viruses%2C%20and%20Trojans%20from%20entering%20and%20infecting%20a%20network)
Also here -<https://www.checkpoint.com/downloads/products/antivirus-datasheet.pdf>

NEW QUESTION 31

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 32

In Unified SmartConsole Gateways and Servers tab you can perform the following functions EXCEPT _____.

- A. Upgrade the software version
- B. Open WebUI
- C. Open SSH
- D. Open service request with Check Point Technical Support

Answer: C

NEW QUESTION 34

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 39

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 43

What is the main difference between Static NAT and Hide NAT?

- A. Static NAT only allows incoming connections to protect your network.
- B. Static NAT allow incoming and outgoing connection
- C. Hide NAT only allows outgoing connections.
- D. Static NAT only allows outgoing connection
- E. Hide NAT allows incoming and outgoing connections.
- F. Hide NAT only allows incoming connections to protect your network.

Answer: B

Explanation:

Hide NAT only translates the source address to hide it behind a gateway.

NEW QUESTION 45

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 47

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

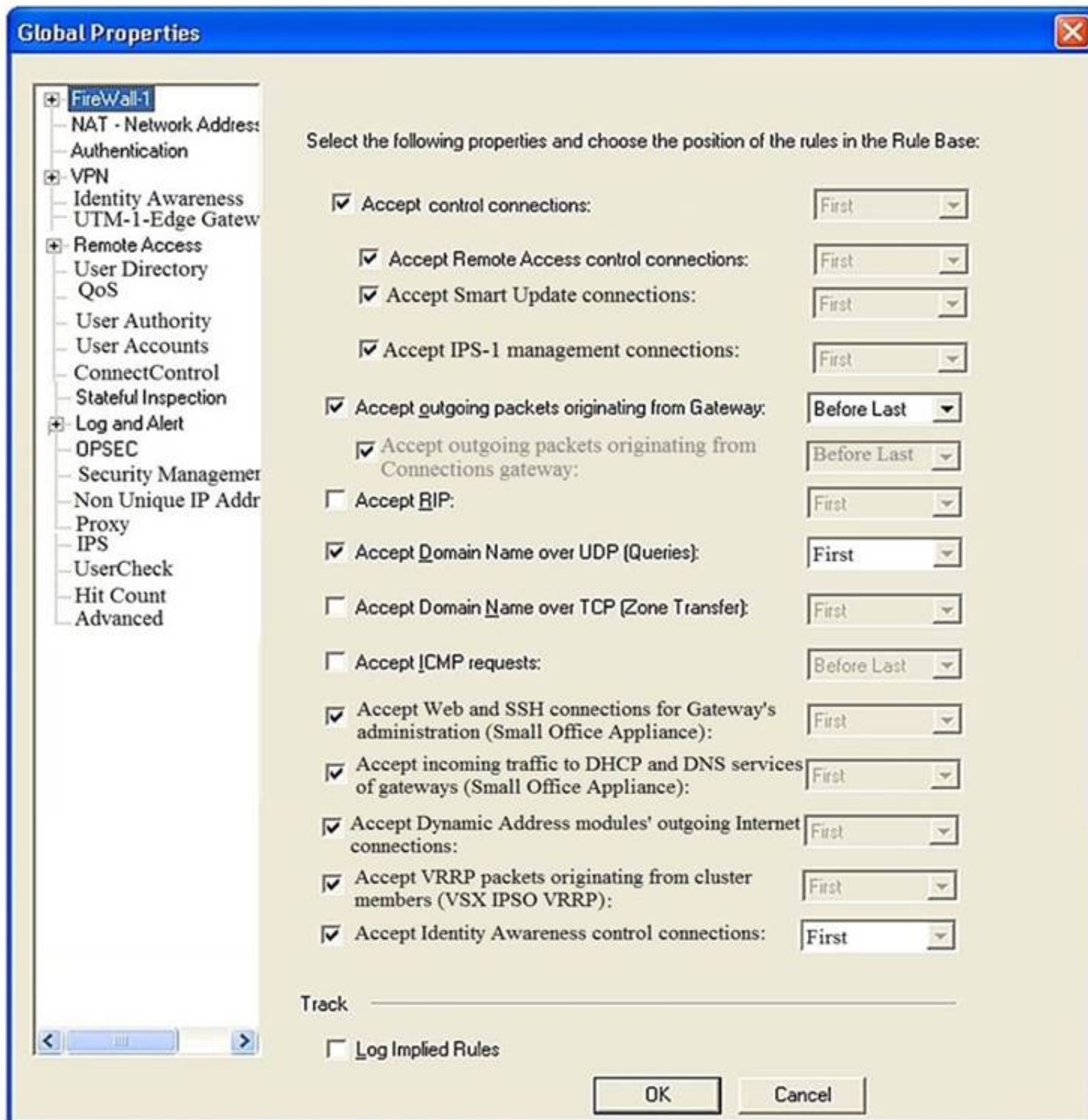
Answer: C

Explanation:

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

NEW QUESTION 51

Consider the Global Properties following settings:



Global Properties

Select the following properties and choose the position of the rules in the Rule Base:

Property	Position
<input checked="" type="checkbox"/> Accept control connections:	First
<input checked="" type="checkbox"/> Accept Remote Access control connections:	First
<input checked="" type="checkbox"/> Accept Smart Update connections:	First
<input checked="" type="checkbox"/> Accept IPS-1 management connections:	First
<input checked="" type="checkbox"/> Accept outgoing packets originating from Gateway:	Before Last
<input checked="" type="checkbox"/> Accept outgoing packets originating from Connections gateway:	Before Last
<input type="checkbox"/> Accept RIP:	First
<input checked="" type="checkbox"/> Accept Domain Name over UDP (Queries):	First
<input type="checkbox"/> Accept Domain Name over TCP (Zone Transfer):	First
<input type="checkbox"/> Accept ICMP requests:	Before Last
<input checked="" type="checkbox"/> Accept Web and SSH connections for Gateway's administration (Small Office Appliance):	First
<input checked="" type="checkbox"/> Accept incoming traffic to DHCP and DNS services of gateways (Small Office Appliance):	First
<input checked="" type="checkbox"/> Accept Dynamic Address modules' outgoing Internet connections:	First
<input checked="" type="checkbox"/> Accept VRRP packets originating from cluster members (VSX IPSO VRRP):	First
<input checked="" type="checkbox"/> Accept Identity Awareness control connections:	First

Track ☒ Log Implied Rules

OK Cancel

The selected option "Accept Domain Name over UDP (Queries)" means:

- A. UDP Queries will be accepted by the traffic allowed only through interfaces with external anti-spoofing topology and this will be done before first explicit rule written by Administrator in a Security Policy.
- B. All UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
- C. No UDP Queries will be accepted by the traffic allowed through all interfaces and this will be done before first explicit rule written by Administrator in a Security Policy.
- D. All UDP Queries will be accepted by the traffic allowed by first explicit rule written by Administrator in a Security Policy.

Answer: A

NEW QUESTION 52

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 RestoreThese options let you: To back up a configuration:
The Backup window opens.

NEW QUESTION 57

Check Point licenses come in two forms. What are those forms?

- A. Central and Local.
- B. Access Control and Threat Prevention.
- C. On-premise and Public Cloud.
- D. Security Gateway and Security Management.

Answer: A

NEW QUESTION 59

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 64









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 67

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 presen
- E. Click the pen symbol in order to gain the lock.

Answer: B

NEW QUESTION 71

Where is the “Hit Count” feature enabled or disabled in SmartConsole?

- A. On the Policy Package
- B. On each Security Gateway
- C. On the Policy layer
- D. In Global Properties for the Security Management Server

Answer: B

Explanation:

References:

NEW QUESTION 75

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 80

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 83

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

- A. All-in-one (stand-alone)
- B. CloudGuard
- C. Distributed
- D. Bridge Mode

Answer: B

NEW QUESTION 84

What is the purpose of a Clean-up Rule?

- A. Clean-up Rules do not server any purpose.
- B. Provide a metric for determining unnecessary rules.
- C. To drop any traffic that is not explicitly allowed.
- D. Used to better optimize a policy.

Answer: C

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 89

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 94

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 97

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 102

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 104

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 109

Which Check Point software blade monitors Check Point devices and provides a picture of network and security performance?

- A. Application Control
- B. Threat Emulation
- C. Logging and Status
- D. Monitoring

Answer: D

Explanation:

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

NEW QUESTION 111

How can the changes made by an administrator before publishing the session be seen by a superuser administrator?

- A. By impersonating the administrator with the 'Login as...' option
- B. They cannot be seen
- C. From the SmartView Tracker audit log
- D. From Manage and Settings > Sessions, right click on the session and click 'View Changes...'

Answer: D

Explanation:

From the Smartconsole, you can possibly view the changes via Manage & setting, Sessions

NEW QUESTION 115

What are the Threat Prevention software components available on the Check Point Security Gateway?

- A. IPS, Threat Emulation and Threat Extraction
- B. IPS, Anti-Bot, Anti-Virus, SandBlast and Macro Extraction
- C. IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction
- D. IDS, Forensics, Anti-Virus, Sandboxing

Answer: C

NEW QUESTION 120

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 121

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 122

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 123

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 128

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 133

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 135

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 140

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 143

Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 148

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 153

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 158

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 162

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 165

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 166

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

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

Answer: A

NEW QUESTION 171

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 175

To view the policy installation history for each gateway, which tool would an administrator use?

- A. Revisions
- B. Gateway installations
- C. Installation history
- D. Gateway history

Answer: C

NEW QUESTION 180

Which Threat Prevention profile uses sanitization technology?

- A. Cloud/data Center
- B. perimeter
- C. Sandbox
- D. Guest Network

Answer: B

Explanation:

Strict Security for Perimeter Profile & Perimeter Profile use sanitization as a technology in Threat prevention profile

NEW QUESTION 181

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 186

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 188

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 189

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 191

Gaia includes Check Point Upgrade Service Engine (CPUSE), which can directly receive updates for what components?

- A. The Security Gateway (SG) and Security Management Server (SMS) software and the CPUSE engine.
- B. Licensed Check Point products for the Gaia operating system and the Gaia operating system itself.
- C. The CPUSE engine and the Gaia operating system.
- D. The Gaia operating system only.

Answer: B

Explanation:

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

NEW QUESTION 196

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 201

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 206

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 208

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

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

Answer: B

NEW QUESTION 211

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 216

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 219

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 221

What is the main objective when using Application Control?

- A. To filter out specific content.
- B. To assist the firewall blade with handling traffic.
- C. To see what users are doing.
- D. Ensure security and privacy of information.

Answer: A

Explanation:

<https://www.checkpoint.com/cyber-hub/network-security/what-is-application-control/>

NEW QUESTION 222

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- A. Symmetric routing
- B. Failovers
- C. Asymmetric routing
- D. Anti-Spoofing

Answer: B

NEW QUESTION 227

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 228

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 230

When defining group-based access in an LDAP environment with Identity Awareness, what is the BEST object type to represent an LDAP group in a Security

Policy?

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

Answer: A

NEW QUESTION 235

In order for changes made to policy to be enforced by a Security Gateway, what action must an administrator perform?

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

Answer: C

NEW QUESTION 236

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 238

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 243

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 246

Which software blade enables Access Control policies to accept, drop, or limit web site access based on user, group, and/or machine?

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

Answer: A

NEW QUESTION 247

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 251

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 255

What are the three deployment considerations for a secure network?

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

Answer: A

NEW QUESTION 258

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

- A. Shared secret
- B. Token
- C. Username/password or Kerberos Ticket
- D. Certificate

Answer: C

Explanation:

Two ways of auth: Username/Password in Captive Portal or Transparent Kerberos Auth through Kerberos Ticket.
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_IdentityAwareness_AdminGuide/T

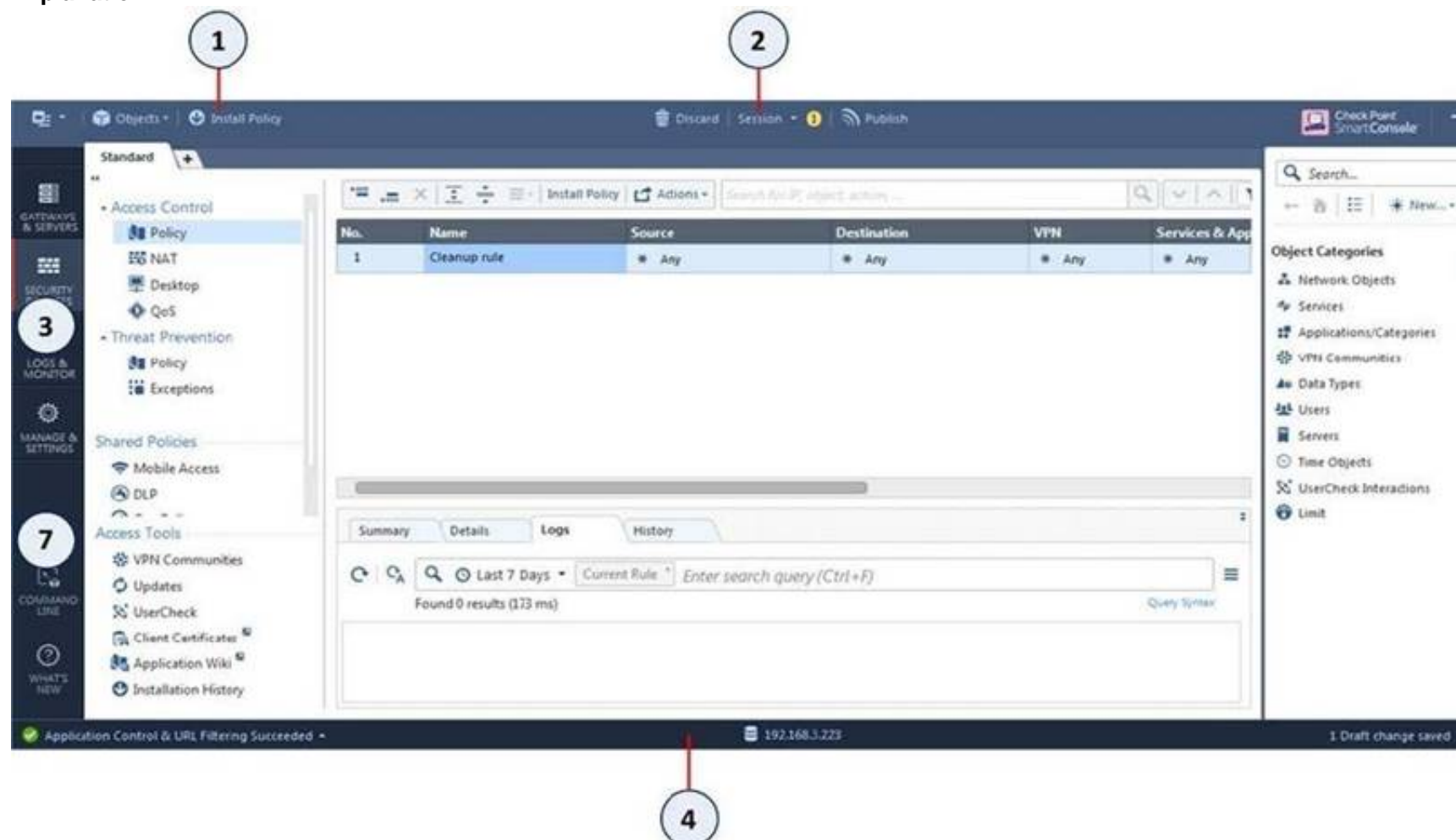
NEW QUESTION 259

Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

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

Answer: A

Explanation:



Item	Description
1	Global Toolbar
2	Session Management Toolbar
3	Navigation Toolbar
4	System Information Area

Item	Description
5	Objects Bar (F11)
6	Validations pane
7	Command line interface button

NEW QUESTION 260

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 264

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 266

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 270

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 271

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 identifies 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 276

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 280

What command would show the API server status?

- A. cpm status
- B. api restart
- C. api status
- D. show api status

Answer: D

NEW QUESTION 285

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 289

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 291

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

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

Answer: C

NEW QUESTION 292

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 293

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 297

True or False: More than one administrator can log into the Security Management Server with SmartConsole with write permission at the same time.

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

Answer: C

Explanation:

Multiple R/W admins can log into SmartConsole and edit rules but they can't edit a rule that is being worked on by another admin.

NEW QUESTION 300

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 303

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 308

.....

Relate Links

100% Pass Your 156-215.81 Exam with Exambible Prep Materials

<https://www.exambible.com/156-215.81-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>