



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

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

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

Answer: B

NEW QUESTION 2

Which of the following are types of VPN communities?

- A. Pentagon, star, and combination
- B. Star, octagon, and combination
- C. Combined and star
- D. Meshed, star, and combination

Answer: D

NEW QUESTION 3

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 4

What is the purpose of the Stealth Rule?

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

Answer: A

NEW QUESTION 5

What are the two types of NAT supported by the Security Gateway?

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

Answer: B

Explanation:

A Security Gateway can use these procedures to translate IP addresses in your network:

NEW QUESTION 6

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 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

Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

- A. Go to clash-Run cpstop | Run cpstart
- B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
- C. Administrator does not need to perform any tas
- D. Check Point will make use of the newly installed CPU and Cores
- E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer: B

NEW QUESTION 9

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 10

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 10

Name one limitation of using Security Zones in the network?

- A. Security zones will not work in Automatic NAT rules
- B. Security zone will not work in Manual NAT rules
- C. Security zones will not work in firewall policy layer
- D. Security zones cannot be used in network topology

Answer: B

Explanation:

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

NEW QUESTION 11

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 15

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 17

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 19

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 23

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 24

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 25

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 27

Which of the following is NOT a tracking log option in R80.x?

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

Answer: C

NEW QUESTION 32

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 36

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 40

When a SAM rule is required on Security Gateway to quickly block suspicious connections which are not restricted by the Security Policy, what actions does the administrator need to take?

- A. SmartView Monitor should be opened and then the SAM rule/s can be applied immediately
- B. Installing policy is not required.
- C. The policy type SAM must be added to the Policy Package and a new SAM rule must be applied. Simply Publishing the changes applies the SAM rule on the firewall.
- D. The administrator must work on the firewall CLI (for example with SSH and PuTTY) and the command 'sam block' must be used with the right parameters.
- E. The administrator should open the LOGS & MONITOR view and find the relevant log
- F. Right clicking on the log entry will show the Create New SAM rule option.

Answer: A

Explanation:

A Security Gateway with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policy. These rules are applied immediately (policy installation is not required).

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide

NEW QUESTION 42

Core Protections are installed as part of what Policy?

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

Answer: A

Explanation:

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

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

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

NEW QUESTION 47

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 51

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 53

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

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

Answer: B

NEW QUESTION 54

Identify the ports to which the Client Authentication daemon listens on by default?

- A. 259, 900
- B. 256, 257
- C. 8080, 529
- D. 80, 256

Answer: A

NEW QUESTION 56

Which of the following is NOT a tracking option? (Select three)

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

Answer: ACD

NEW QUESTION 57

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 58

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 59

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 60

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 61

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

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

Answer: D

Explanation:

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

NEW QUESTION 64

Both major kinds of NAT support Hide and Static NAT. However, one offers more flexibility. Which statement is true?

- A. Manual NAT can offer more flexibility than Automatic NAT.
- B. Dynamic Network Address Translation (NAT) Overloading can offer more flexibility than Port Address Translation.
- C. Dynamic NAT with Port Address Translation can offer more flexibility than Network Address Translation (NAT) Overloading.
- D. Automatic NAT can offer more flexibility than Manual NAT.

Answer: A

Explanation:

"An Auto-NAT rule only uses the source address and port when matching and translating. Manual NAT can match and translate source and destination addresses and ports." <https://networkdirection.net/articles/firewalls/firepowermanagementcentre/fmcnatpolicies/>

NEW QUESTION 67

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

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

Answer: B

NEW QUESTION 70

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 72

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 73

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 75

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 79

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 83

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 88

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

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

Answer: B

NEW QUESTION 90

You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

- A. fw ctl multik dynamic_dispatching on
- B. fw ctl multik dynamic_dispatching set_mode 9
- C. fw ctl multik set_mode 9
- D. fw ctl multik pq enable

Answer: C

NEW QUESTION 92

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 97

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 99

What is the purpose of Captive Portal?

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

Answer: C

Explanation:

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

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

NEW QUESTION 104

What 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 108

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

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

Answer: B

NEW QUESTION 109

How many layers make up the TCP/IP model?

- A. 2
- B. 7
- C. 6
- D. 4

Answer: D

NEW QUESTION 113

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 115

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 118

In _____ NAT, the _____ is translated.

- A. Hide; source

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

Answer: A

NEW QUESTION 120

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 122

To increase security, the administrator has modified the Core protection 'Host Port Scan' from 'Medium' to 'High' Predefined Sensitivity. Which Policy should the administrator install after Publishing the changes?

- A. The Access Control and Threat Prevention Policies.
- B. The Access Control Policy.
- C. The Access Control & HTTPS Inspection Policy.
- D. The Threat Prevention Policy.

Answer: D

Explanation:

<https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubm>

NEW QUESTION 125

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 130

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

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

Answer: B

NEW QUESTION 133

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 137

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

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

Answer: C

Explanation:

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

NEW QUESTION 140

A stateful inspection firewall works by registering connection data and compiling this information. Where is the information stored?

- A. In the system SMEM memory pool.
- B. In State tables.
- C. In the Sessions table.
- D. In a CSV file on the firewall hard drive located in \$FWDIR/conf/.

Answer: B

Explanation:

The information stored in the state tables provides cumulative data that can be used to evaluate future connections.....
<https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-a-stateful-firewall/>

NEW QUESTION 143

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 144

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 145

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 147

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 150

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 155

Application Control/URL filtering database library is known as:

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

Answer: B

Explanation:

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

NEW QUESTION 158

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 163

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 167

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

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

Answer: A

NEW QUESTION 172

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

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

Answer: A

NEW QUESTION 176

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 180

What are the three components for Check Point Capsule?

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

Answer: D

NEW QUESTION 183

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 186

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

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

Answer: D

Explanation:

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

NEW QUESTION 189

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 190

What kind of NAT enables Source Port Address Translation by default?

- A. Automatic Static NAT
- B. Manual Hide NAT
- C. Automatic Hide NAT
- D. Manual Static NAT

Answer: C

Explanation:

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

NEW QUESTION 193

The Online Activation method is available for Check Point manufactured appliances. How does the administrator use the Online Activation method?

- A. The SmartLicensing GUI tool must be launched from the SmartConsole for the Online Activation tool to start automatically.
- B. No action is required if the firewall has internet access and a DNS server to resolve domain names.
- C. Using the Gaia First Time Configuration Wizard, the appliance connects to the Check Point User Center and downloads all necessary licenses and contracts.
- D. The cpinfo command must be run on the firewall with the switch -online-license-activation.

Answer: C

Explanation:

"Online activation: this method of activation is available for Check Point manufactured appliances. These appliances should be configured to have internet connectivity during the completion of the First Time Configuration Wizard for software version R77 and below. Customers using R80 and higher will be able to use this feature during or after the completion of the First Time Configuration Wizard."

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

NEW QUESTION 196

What is the RFC number that act as a best practice guide for NAT?

- A. RFC 1939
- B. RFC 1950
- C. RFC 1918
- D. RFC 793

Answer: C

Explanation:

<https://datatracker.ietf.org/doc/html/rfc1918>

NEW QUESTION 200

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 202

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 206

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 211

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 216

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 218

What are the three types of UserCheck messages?

- A. inform, ask, and block
- B. block, action, and warn
- C. action, inform, and ask
- D. ask, block, and notify

Answer: A

Explanation:

Inform User Inform

Shows when the action for the ruleClosed is inform. It informs users what the company policy is for that site. Blocked Message

Block

Shows when a request is blocked. Ask User

Ask

Shows when the action for the rule is ask. It informs users what the company policy is for that site and they must click OK to continue to the site.

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_DataLossPrevention_AdminGuide/

NEW QUESTION 219

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

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

Answer: D

Explanation:

The snapshot creates a binary image of the entire root (lv_current) disk partition. This includes Check Point products, configuration, and operating system. Starting in R77.10, exporting an image from one machine and importing that image on another machine of the same type is supported. The log partition is not included in the snapshot. Therefore, any locally stored FireWall logs will not be save

NEW QUESTION 220

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 222

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

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

Answer: A

NEW QUESTION 225

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 229

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 232

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 234

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

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

Answer: B

Explanation:

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

NEW QUESTION 236

In the Check Point Security Management Architecture, which component(s) can store logs?

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

Answer: B

NEW QUESTION 237

Which type of attack can a firewall NOT prevent?

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

Answer: A

NEW QUESTION 239

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 240

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

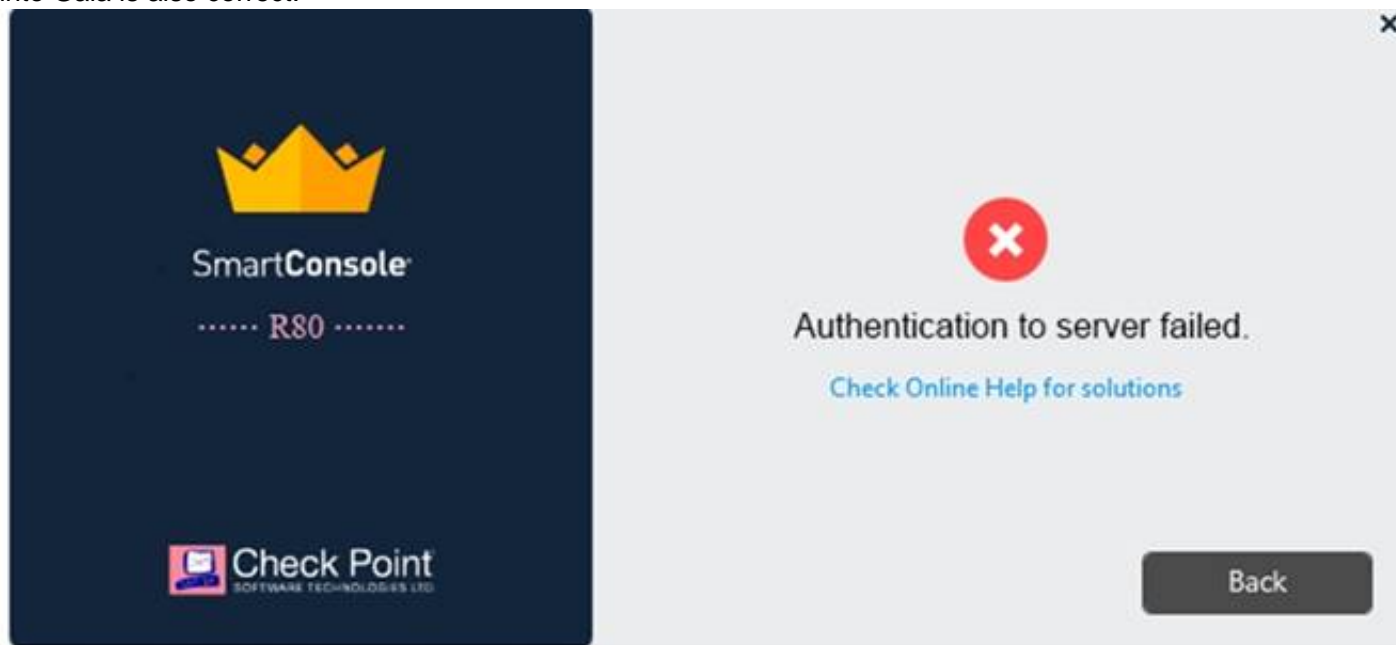
Explanation:

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 245

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 SmartConsol

- 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 249

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

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

Answer: B

Explanation:

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

NEW QUESTION 250

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

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

Answer: A

NEW QUESTION 254

A 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 255

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 257

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

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

Answer: B

NEW QUESTION 261

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 265

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

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

Answer: A

NEW QUESTION 268

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 269

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 272

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 273

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 276

Which of the following Windows Security Events will NOT map a username to an IP address in Identity Awareness?

- A. Kerberos Ticket Renewed
- B. Kerberos Ticket Requested
- C. Account Logon
- D. Kerberos Ticket Timed Out

Answer: D

NEW QUESTION 277

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 279

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 282

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 283

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 287

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 288

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 291

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 296

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 297

Fill in the blank: SmartConsole, SmartEvent GUI client, and _____ allow viewing of billions of consolidated logs and shows them as prioritized security events.

- A. SmartView Web Application
- B. SmartTracker
- C. SmartMonitor
- D. SmartReporter

Answer: A

Explanation:

"The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents"

https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=docume

NEW QUESTION 301

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

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

Answer: B

NEW QUESTION 305

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 309

How do you manage Gaia?

- A. Through CLI and WebUI
- B. Through CLI only
- C. Through SmartDashboard only
- D. Through CLI, WebUI, and SmartDashboard

Answer: D

NEW QUESTION 311

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 313

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

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

Answer: D

NEW QUESTION 314

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

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

Answer: C

Explanation:

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

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

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

NEW QUESTION 316

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 319

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 323

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 327

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 328

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 332

Security Zones do not work with what type of defined rule?

- A. Application Control rule
- B. Manual NAT rule
- C. IPS bypass rule
- D. Firewall rule

Answer: B

Explanation:

<https://community.checkpoint.com/t5/Management/Workaround-for-manual-NAT-when-security-zones-are-use>

NEW QUESTION 335

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

- A. remote access clients.
- B. a combination of computer or computer groups and networks.
- C. users and user groups.
- D. All of the above.

Answer: D

Explanation:

To create an access role:

The Access Role window opens.

Your selection is shown in the Networks node in the Role Preview pane.

A window opens. You can search for Active Directory entries or select them from the list. You can search for AD entries or select them from the list.

The access role is added to the Users and Administrators tree.

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

NEW QUESTION 339

Secure Internal Communication (SIC) is handled by what process?

- A. CPM
- B. HTTPS
- C. FWD
- D. CPD

Answer: D

Explanation:

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

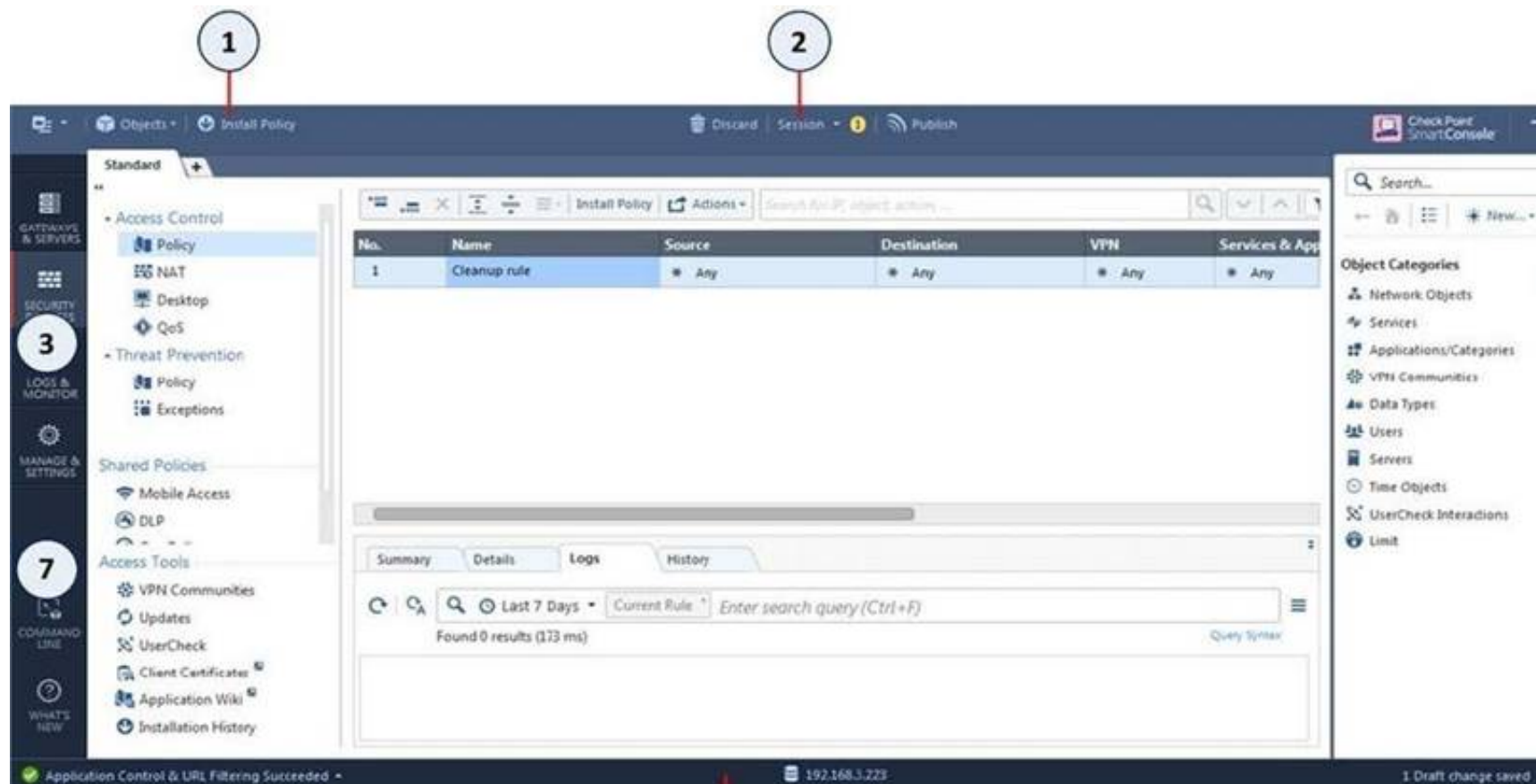
NEW QUESTION 342

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 346

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 350

To view statistics on detected threats, which Threat Tool would an administrator use?

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

Answer: D

NEW QUESTION 351

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 356

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 359

When configuring Anti-Spoofing, which tracking options can an Administrator select?

- A. Log, Alert, None
- B. Log, Allow Packets, Email
- C. Drop Packet, Alert, None
- D. Log, Send SNMP Trap, Email

Answer: A

Explanation:

Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected: Log - Create a log entry (default)

Alert - Show an alert None - Do not log or alert

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

NEW QUESTION 361

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 363

How Capsule Connect and Capsule Workspace differ?

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

Answer: A

NEW QUESTION 368

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 371

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 374

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 375

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 377

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 378

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 381

Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _____.

- A. On all satellite gateway to satellite gateway tunnels
- B. On specific tunnels for specific gateways
- C. On specific tunnels in the community
- D. On specific satellite gateway to central gateway tunnels

Answer: C

Explanation:

Each VPN tunnel in the community may be set to be a Permanent Tunnel. Since Permanent Tunnels are constantly monitored, if the VPN tunnel is down, then a log, alert, or user defined action, can be issued. A VPN tunnel is monitored by periodically sending "tunnel test" packets. As long as responses to the packets are received the VPN tunnel is considered "up." If no response is received within a given time period, the VPN tunnel is considered "down." Permanent Tunnels can only be established between Check Point Security Gateways. The configuration of Permanent Tunnels takes place on the community level and:

NEW QUESTION 384

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 387

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 391

Which repositories are installed on the Security Management Server by SmartUpdate?

- A. License and Update
- B. Package Repository and Licenses
- C. Update and License & Contract
- D. License & Contract and Package Repository

Answer: D

Explanation:

References:

NEW QUESTION 394

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 397

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

- A. Identity Awareness is not enabled.
- B. Log Trimming is enabled.
- C. Logging has disk space issues
- D. Content Awareness is not enabled.

Answer: D

NEW QUESTION 402

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 404

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

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

Answer: A

Explanation:

Phase I modes

Between Security Gateways, there are two modes for IKE phase I. These modes only apply to IKEv1:

NEW QUESTION 406

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

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

Answer: B

Explanation:

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

NEW QUESTION 410

Name the authentication method that requires token authenticator.

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

Answer: A

Explanation:

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

NEW QUESTION 412

What is UserCheck?

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

Answer: B

Explanation:

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

NEW QUESTION 413

.....

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/>