

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

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



NEW QUESTION 1

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 2

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

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

Answer: D

Explanation:

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

NEW QUESTION 3

What is the purpose of the Stealth Rule?

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

Answer: A

NEW QUESTION 4

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 5

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 6

The default shell of the Gaia CLI is cli.sh. How do you change from the cli.sh shell to the advanced shell to run Linux commands?

- A. Execute the command 'enable' in the cli.sh shell
- B. Execute the 'conf t' command in the cli.sh shell
- C. Execute the command 'expert' in the cli.sh shell
- D. Execute the 'exit' command in the cli.sh shell

Answer: C

NEW QUESTION 7

Under which file is the proxy arp configuration stored?

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

Answer: D

NEW QUESTION 8

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 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

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 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

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 22

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 24

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 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 30

What is the purpose of the Clean-up Rule?

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

Answer: A

Explanation:

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

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

NEW QUESTION 34

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

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

Answer: B

Explanation:

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

NEW QUESTION 35

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 40

To provide updated malicious data signatures to all Threat Prevention blades, the Threat Prevention gateway does what with the data?

- A. Cache the data to speed up its own function.
- B. Share the data to the ThreatCloud for use by other Threat Prevention blades.
- C. Log the traffic for Administrator viewing.
- D. Delete the data to ensure an analysis of the data is done each time.

Answer: B

Explanation:

Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the ThreatCloud for use by the other Threat Prevention blades. src

<https://infosec.co.il/wp-content/uploads/2020/06/12-GAiA-R80.40-Threat-Prevention.pdf> page 28.

NEW QUESTION 43

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

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

Answer: D

NEW QUESTION 47

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 Closed 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 52

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](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%22)

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 56

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 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 61

Which command shows the installed licenses?

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

Answer: A

NEW QUESTION 66

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 68

What is the SOLR database for?

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

Answer: A

NEW QUESTION 71

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 74

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

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

Answer: B

NEW QUESTION 75

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 78

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 82

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 84

Rugged appliances are small appliances with ruggedized hardware and like Quantum Spark appliance they use which operating system?

- A. Centos Linux
- B. Gaia embedded
- C. Gaia
- D. Red Hat Enterprise Linux version 5

Answer: B

Explanation:

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

NEW QUESTION 86

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 91

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 96

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 101

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 105

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

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

Answer: B

NEW QUESTION 110

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

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

Answer: B

NEW QUESTION 115

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 117

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 118

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

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

Answer: C

NEW QUESTION 123

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 127

In order to modify Security Policies the administrator can use which of the following tools? (Choose the best answer.)

- A. SmartConsole and WebUI on the Security Management Server.
- B. SmartConsole or mgmt_cli (API) on any computer where SmartConsole is installed.
- C. Command line of the Security Management Server or mgmt_cli.exe on any Windows computer.
- D. mgmt_cli (API) or WebUI on Security Gateway and SmartConsole on the Security Management Server.

Answer: B

NEW QUESTION 132

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 136

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 140

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 144

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 145

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 149

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 150

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

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

Answer: D

NEW QUESTION 152

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

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

Answer: D

NEW QUESTION 156

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 159

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 162

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 165

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

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

Answer: D

NEW QUESTION 166

Which of the following is considered to be the more secure and preferred VPN authentication method?

- A. Password
- B. Certificate
- C. MD5
- D. Pre-shared secret

Answer: B

Explanation:

References:

NEW QUESTION 171

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 172

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 173

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 175

How would you determine the software version from the CLI?

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

Answer: A

NEW QUESTION 177

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 178

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

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

Answer: C

NEW QUESTION 180

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

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

Answer: B

NEW QUESTION 181

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 183

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

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

Answer: B

NEW QUESTION 184

Which of the following describes how Threat Extraction functions?

- A. Detect threats and provides a detailed report of discovered threats
- B. Proactively detects threats
- C. Delivers file with original content
- D. Delivers PDF versions of original files with active content removed

Answer: B

NEW QUESTION 185

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 186

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 189

Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 194

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?eventsubmit_dogoviewsolutiondetails=&solutionid=s

NEW QUESTION 199

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 204

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 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 210

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 211

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

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

Answer: D

NEW QUESTION 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 220

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 224

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 226

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

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

Answer: C

NEW QUESTION 227

After a new Log Server is added to the environment and the SIC trust has been established with the SMS what will the gateways do?

- A. The gateways can only send logs to an SMS and cannot send logs to a Log Serve
- B. Log Servers are proprietary log archive servers.
- C. Gateways will send new firewall logs to the new Log Server as soon as the SIC trust is set up between the SMS and the new Log Server.
- D. The firewalls will detect the new Log Server after the next policy install and redirect the new logs to the new Log Server.
- E. Logs are not automatically forwarded to a new Log Serve
- F. SmartConsole must be used to manually configure each gateway to send its logs to the server.

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf
https://sc1.checkpoint.com/documents/SMB_R80.20/AdminGuides/Locally_Managed/EN/Content/Topics/Conf

NEW QUESTION 228

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

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

Answer: B

NEW QUESTION 233

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

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

Answer: B

NEW QUESTION 238

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

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

Answer: C

NEW QUESTION 240

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

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

Answer: B

NEW QUESTION 245

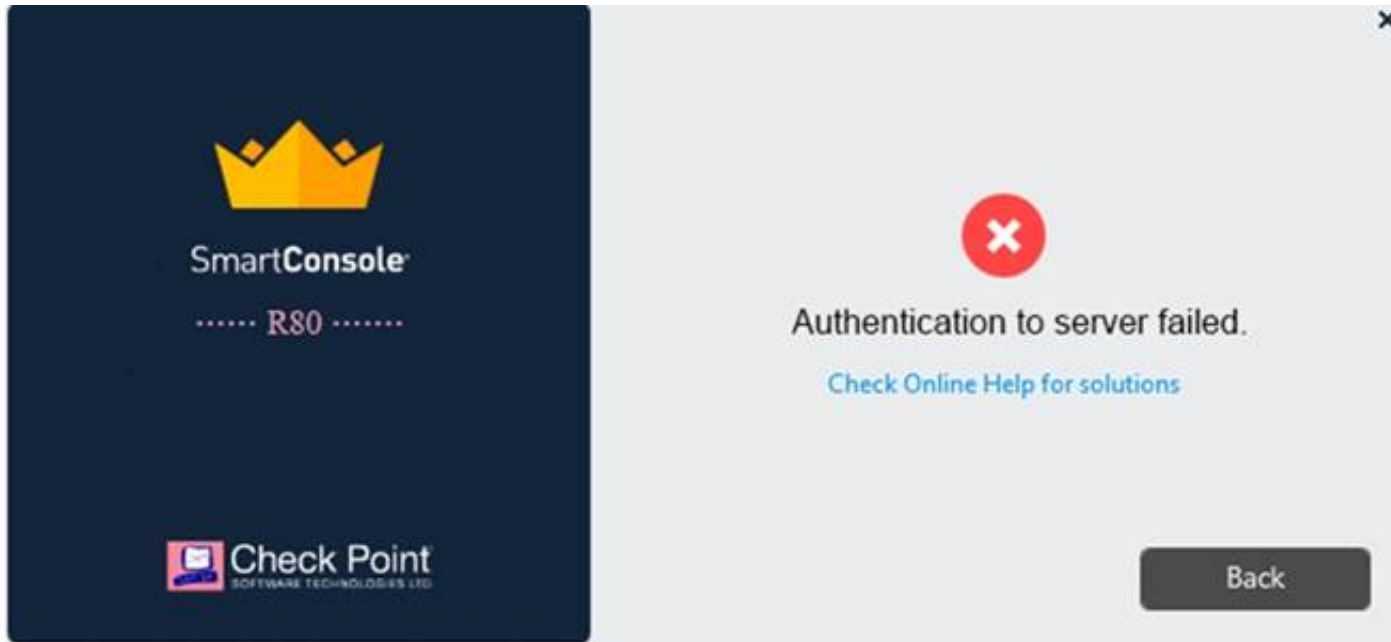
In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- A. SND is a feature to accelerate multiple SSL VPN connections
- B. SND is an alternative to IPSec Main Mode, using only 3 packets
- C. SND is used to distribute packets among Firewall instances
- D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

NEW QUESTION 248

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



What is the most likely reason?

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

Answer: B

NEW QUESTION 253

Which statement is TRUE of anti-spoofing?

- A. Anti-spoofing is not needed when IPS software blade is enabled
- B. It is more secure to create anti-spoofing groups manually
- C. It is BEST Practice to have anti-spoofing groups in sync with the routing table
- D. With dynamic routing enabled, anti-spoofing groups are updated automatically whenever there is a routing change

Answer: C

NEW QUESTION 258

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 262

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 266

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 267

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

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

Answer: B

NEW QUESTION 271

Name the pre-defined Roles included in Gaia OS.

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

Answer: A

NEW QUESTION 275

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

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

Answer: B

NEW QUESTION 277

URL Filtering cannot be used to:

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

Answer: D

Explanation:

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

NEW QUESTION 278

Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R80 configuration, clean install R80.10 and import the configuration
- B. CPUSE online upgrade
- C. CPUSE offline upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 280

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 281

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 282

When should you generate new licenses?

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

Answer: C

NEW QUESTION 286

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

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

Answer: B

NEW QUESTION 290

What are the three deployment options available for a security gateway?

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

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm

NEW QUESTION 294

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 295

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 299

What command from the CLI would be used to view current licensing?

- A. license view

- B. fw ctl tab -t license -s
- C. show license -s
- D. cplic print

Answer: D

NEW QUESTION 303

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 308

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

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

Answer: B

NEW QUESTION 312

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

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

Answer: A

NEW QUESTION 314

In which deployment is the security management server and Security Gateway installed on the same appliance?

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

Answer: A

Explanation:

<https://www.youtube.com/watch?v=BFNnBKQz5HA>

NEW QUESTION 318

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 321

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 325

What protocol is specifically used for clustered environments?

- A. Clustered Protocol

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

Answer: D

NEW QUESTION 326

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 330

Which of the following is NOT an identity source used for Identity Awareness?

- A. Remote Access
- B. UserCheck
- C. AD Query
- D. RADIUS

Answer: B

NEW QUESTION 335

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 339

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 342

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 345

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 350

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 352

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

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

Answer: D

NEW QUESTION 353

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 357

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

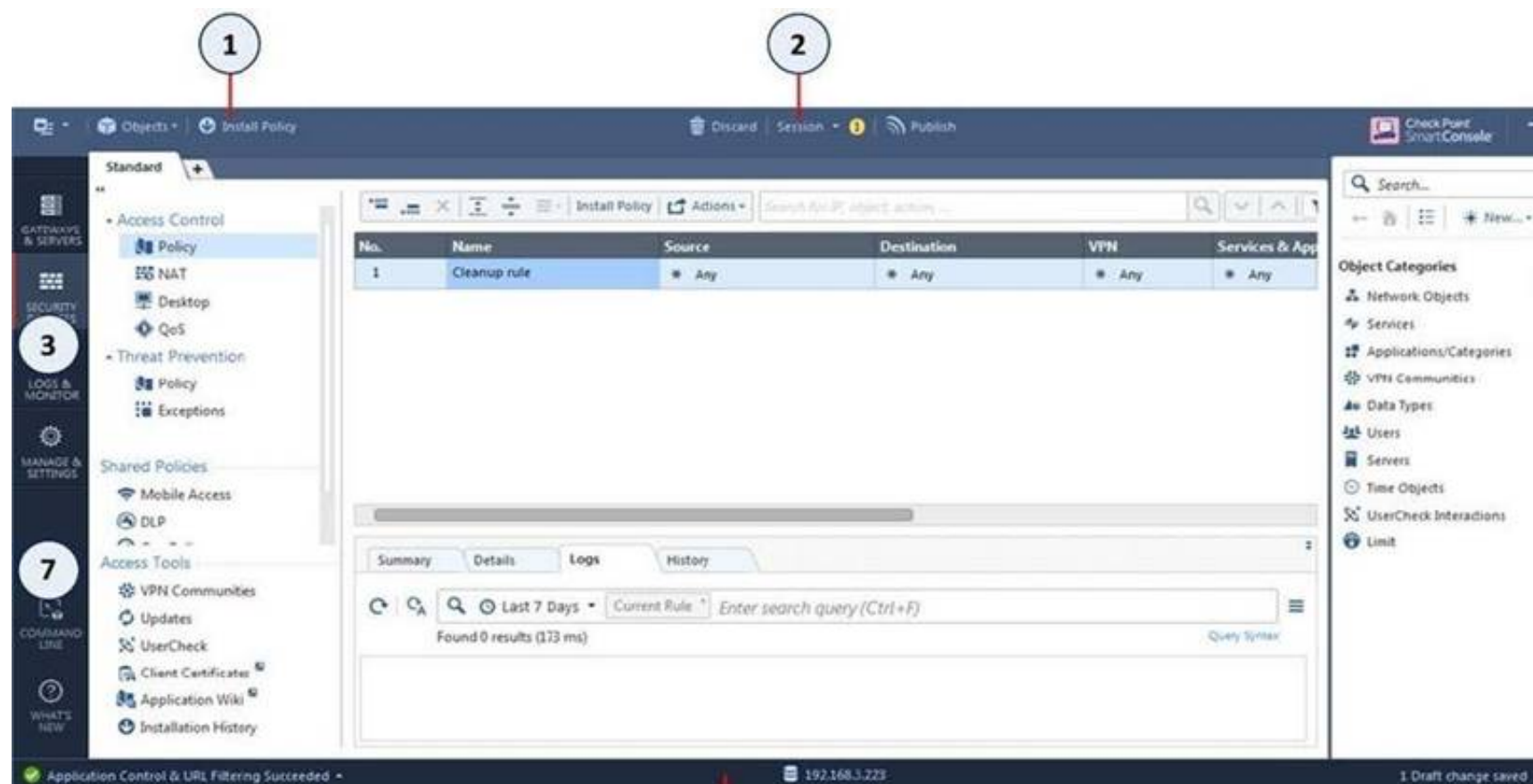
NEW QUESTION 362

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 366

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 371

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 372

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 376

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

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

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

Answer: A

NEW QUESTION 379

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

Answer: D

NEW QUESTION 382

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 385

CPU-level of your Security gateway is peaking to 100% causing problems with traffic. You suspect that the problem might be the Threat Prevention settings. The following Threat Prevention Profile has been created.

Company TP Profile

Provide very wide coverage for all products and protocols, with noticeable performance impact.

General Policy

IPS

Anti-Bot

Anti-Virus

Threat Emulation

Malware DNS Trap

Blades Activation

☒ IPS
 ☒ Anti-Bot
 ☒ Anti-Virus
 ☒ Threat Emulation

Activate Protections

Performance Impact:

Severity:

Activation Mode

High Confidence:

Medium Confidence:

Low Confidence:

OK

Cancel

How could you tune the profile in order to lower the CPU load still maintaining security at good level? Select the BEST answer.

- A. Set High Confidence to Low and Low Confidence to Inactive.
- B. Set the Performance Impact to Medium or lower.
- C. The problem is not with the Threat Prevention Profil
- D. Consider adding more memory to the appliance.
- E. Set the Performance Impact to Very Low Confidence to Prevent.

Answer: B

NEW QUESTION 390

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

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

Answer: D

NEW QUESTION 392

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 393

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 396

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 398

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

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

Answer: B

NEW QUESTION 399

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 403

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 405

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 406

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 411

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 412

Can you use the same layer in multiple policies or rulebases?

- A. Yes - a layer can be shared with multiple policies and rules.
- B. No - each layer must be unique.
- C. No - layers cannot be shared or reused, but an identical one can be created.
- D. Yes - but it must be copied and pasted with a different name.

Answer: A

Explanation:

<https://community.checkpoint.com/t5/Management/Sharing-a-layer-across-different-policies/td-p/1660>

NEW QUESTION 413

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 416

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

156-215.81 Practice Exam Features:

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