



CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

NEW QUESTION 1

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

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

Answer: B

Explanation:

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

NEW QUESTION 2

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

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

Answer: B

NEW QUESTION 3

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 4

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 5

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 6

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 7

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 8

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 9

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

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

Answer: A

Explanation:

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

NEW QUESTION 10

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 10

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 15

Which statement is NOT TRUE about Delta synchronization?

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

Answer: A

NEW QUESTION 19

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 20

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

- A. New Smart-1 appliances double the physical memory install

- B. Indexing Engine indexes logs for faster search results
- C. SmartConsole now queries results directly from the Security Gateway
- D. The amount of logs been store is less than the usual in older versions

Answer: B

Explanation:

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

NEW QUESTION 25

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 30

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 34

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 38

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 40

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 41

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 42

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 46

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 49

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

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

Answer: D

Explanation:

Installing and Publishing

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

After you did this: Publish

Opened a session in SmartConsole and made changes.

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

Install the database

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

Install a policy Changed the Rule Base.

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

NEW QUESTION 51

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 Closed. These rules are applied immediately (policy installation is not required).

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

NEW QUESTION 52

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 53

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

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

Answer: A

NEW QUESTION 57

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 59

Which single Security Blade can be turned on to block both malicious files from being downloaded as well as block websites known to host malware?

- A. Anti-Bot
- B. None - both Anti-Virus and Anti-Bot are required for this
- C. Anti-Virus
- D. None - both URL Filtering and Anti-Virus are required for this.

Answer: C

Explanation:

Prevent Access to Malicious Websites

The Antivirus Software Blade scans outbound URL requests and ensures users do not visit websites that are known to distribute malware.

Stop Incoming Malicious Files

Check Point Antivirus Software Blade prevents and stops threats such as malware, viruses, and Trojans from entering and infecting a network.

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

NEW QUESTION 61

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 64

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 65

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

- A. sysdown
- B. exit
- C. halt

D. shut-down

Answer: C

NEW QUESTION 68

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

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

Answer: B

Explanation:

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

NEW QUESTION 69

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 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 78

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 81

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

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

Answer: A

NEW QUESTION 82

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 86

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

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

Answer: D

NEW QUESTION 90

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 95

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 96

Which information is included in the “Extended Log” tracking option, but is not included in the “Log” tracking option?

- A. file attributes
- B. application information
- C. destination port
- D. data type information

Answer: B

NEW QUESTION 98

Stateful Inspection compiles and registers connections where?

- A. Connection Cache
- B. State Cache
- C. State Table
- D. Network Table

Answer: C

NEW QUESTION 103

What data MUST be supplied to the SmartConsole System Restore window to restore a backup?

- A. Server, Username, Password, Path, Version
- B. Username, Password, Path, Version
- C. Server, Protocol, Username, Password, Destination Path
- D. Server, Protocol, Username, Password, Path

Answer: D

Explanation:

References:

NEW QUESTION 105

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 108

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 111

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

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

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

Answer: B

NEW QUESTION 113

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

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

Answer: D

Explanation:

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

NEW QUESTION 118

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 123

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 127

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 129

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 130

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 132

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

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

Answer: B

NEW QUESTION 133

Which type of Check Point license ties the package license to the IP address of the Security Management Server?

- A. Central
- B. Corporate
- C. Local
- D. Formal

Answer: A

Explanation:

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

NEW QUESTION 134

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 137

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

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

Answer: A

Explanation:

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

NEW QUESTION 140

How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 141

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 145

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

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

Answer: B

NEW QUESTION 146

In _____ NAT, the _____ is translated.

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

Answer: A

NEW QUESTION 151

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 155

Choose what BEST describes users on Gaia Platform.

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

Answer: A

Explanation:

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

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

monitor

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

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

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

NEW QUESTION 157

The “Hit count” feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track

the hits even if the Track option is set to “None”?

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

Answer: D

NEW QUESTION 160

Which message indicates IKE Phase 2 has completed successfully?

- A. Quick Mode Complete
- B. Aggressive Mode Complete
- C. Main Mode Complete
- D. IKE Mode Complete

Answer: A

NEW QUESTION 161

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

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

Answer: D

NEW QUESTION 164

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

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

Answer: A

Explanation:

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

The installation process:

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

NEW QUESTION 168

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

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

Answer: D

Explanation:

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

NEW QUESTION 169

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 172

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 175

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 180

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

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

Answer: D

Explanation:

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

NEW QUESTION 185

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 187

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

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

Answer: C

NEW QUESTION 188

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 189

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 193

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 198

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 203

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 204

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

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

Answer: C

Explanation:

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

NEW QUESTION 207

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 212

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 213

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 214

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

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

Answer: B

NEW QUESTION 218

Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 222

When should you generate new licenses?

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

Answer: C

NEW QUESTION 226

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 229

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 232

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

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

Answer: A

NEW QUESTION 234

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 236

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 241

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 243

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

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

Answer: A

NEW QUESTION 247

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

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

Answer: C

Explanation:

Section titles are only for visual categorization of rules.

NEW QUESTION 248

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 253

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 254

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 257

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 259

In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

- A. Accounting
- B. Suppression
- C. Accounting/Suppression
- D. Accounting/Extended

Answer: C

NEW QUESTION 260

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 261

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

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

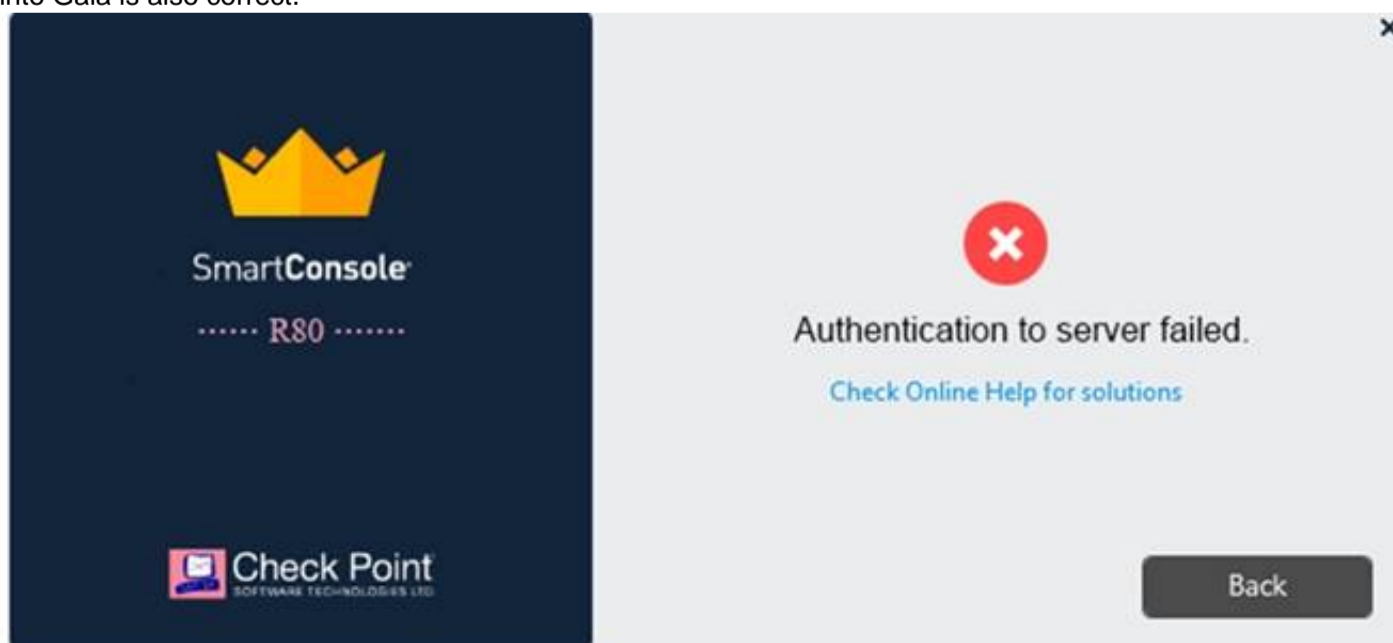
Answer: B

Explanation:

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

NEW QUESTION 265

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 266

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 267

There are four policy types available for each policy package. What are those policy types?

- A. Access Control, Threat Prevention, Mobile Access and HTTPS Inspection
- B. Access Control, Custom Threat Prevention, Autonomous Threat Prevention and HTTPS Inspection
- C. There are only three policy types: Access Control, Threat Prevention and NAT.
- D. Access Control, Threat Prevention, NAT and HTTPS Inspection

Answer: D

Explanation:

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

NEW QUESTION 272

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 273

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 278

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 283

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 284

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 286

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 290

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

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

Answer: A

NEW QUESTION 291

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 293

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 296

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 298

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 302

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 304

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

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

Answer: B

NEW QUESTION 306

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 307

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 315

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 319

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

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

Answer: B

NEW QUESTION 320

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

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

Answer: A

NEW QUESTION 322

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 323

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 327

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

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

Answer: B

NEW QUESTION 332

The SIC Status “Unknown” means

- A. There is connection between the gateway and Security Management Server but it is not trusted.
- B. The secure communication is established.
- C. There is no connection between the gateway and Security Management Server.
- D. The Security Management Server can contact the gateway, but cannot establish SIC.

Answer: C

Explanation:

SIC Status

After the gateway receives the certificate issued by the ICA, the SIC status shows if the Security Management Server can communicate securely with this gateway:

NEW QUESTION 336

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

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

Answer: D

NEW QUESTION 340

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 345

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

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

Answer: C

NEW QUESTION 347

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 348

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

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

Answer: A

Explanation:

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

NEW QUESTION 349

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

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

Answer: A

NEW QUESTION 352

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

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

Answer: B

NEW QUESTION 353

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 355

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

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

Answer: A

NEW QUESTION 360

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 362

Security Zones do no 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 365

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 368

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 370

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 371

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

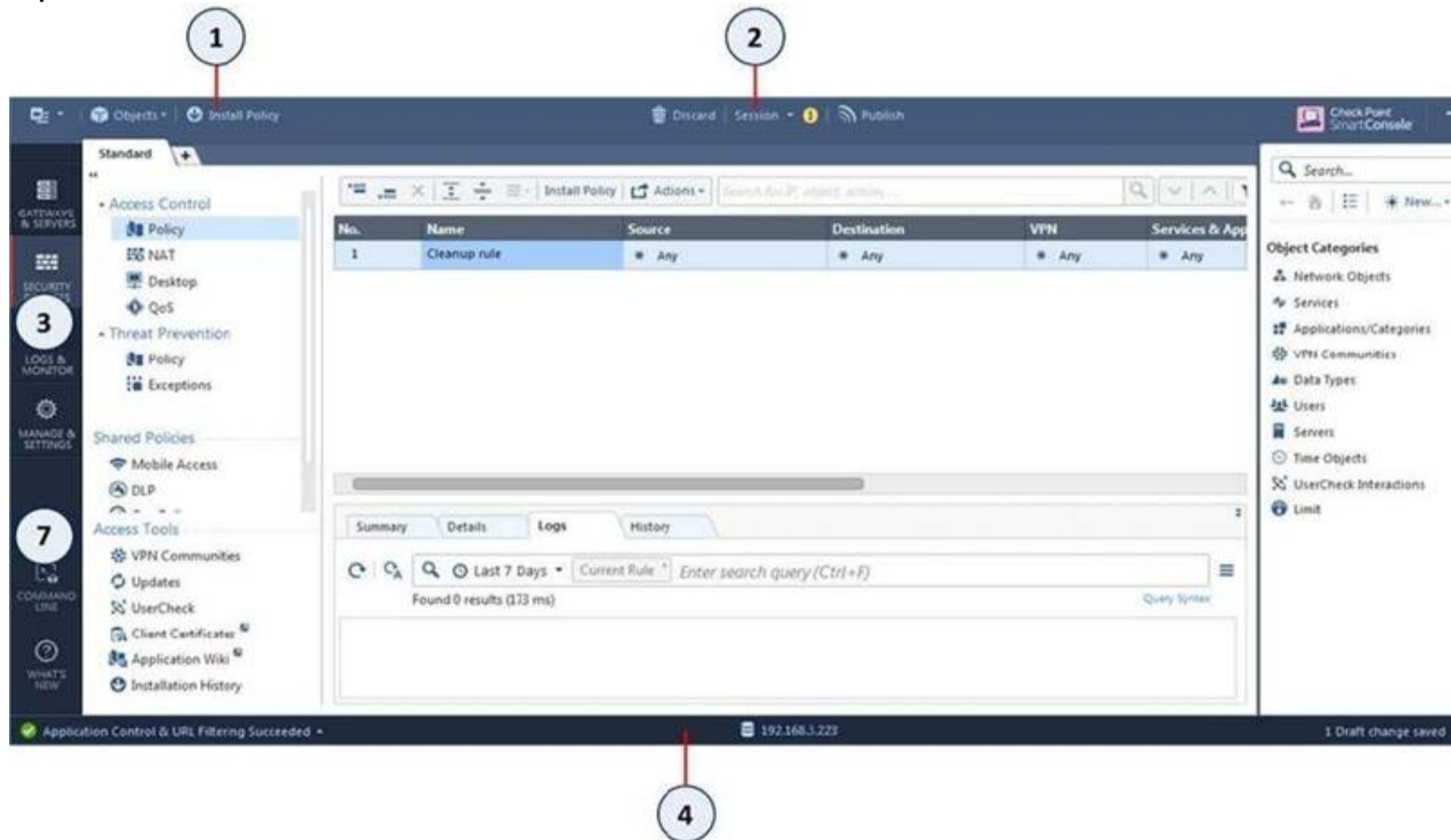
NEW QUESTION 372

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 375

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 380

Which type of Check Point license is tied to the IP address of a specific Security Gateway and cannot be transferred to a gateway that has a different IP address?

- A. Formal
- B. Central
- C. Corporate
- D. Local

Answer: D

Explanation:

Local licensing is associated with the IP address of the Security Gateway, to which the license will be applied.

Each time the IP address of the Security Gateway changes, a new license must be generated and installed.

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

NEW QUESTION 383

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

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

Answer: D

NEW QUESTION 384

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 387

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 390

Which statement describes what Identity Sharing is in Identity Awareness?

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

Answer: C

Explanation:

Identity Sharing

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

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

NEW QUESTION 394

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

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

Answer: C

NEW QUESTION 396

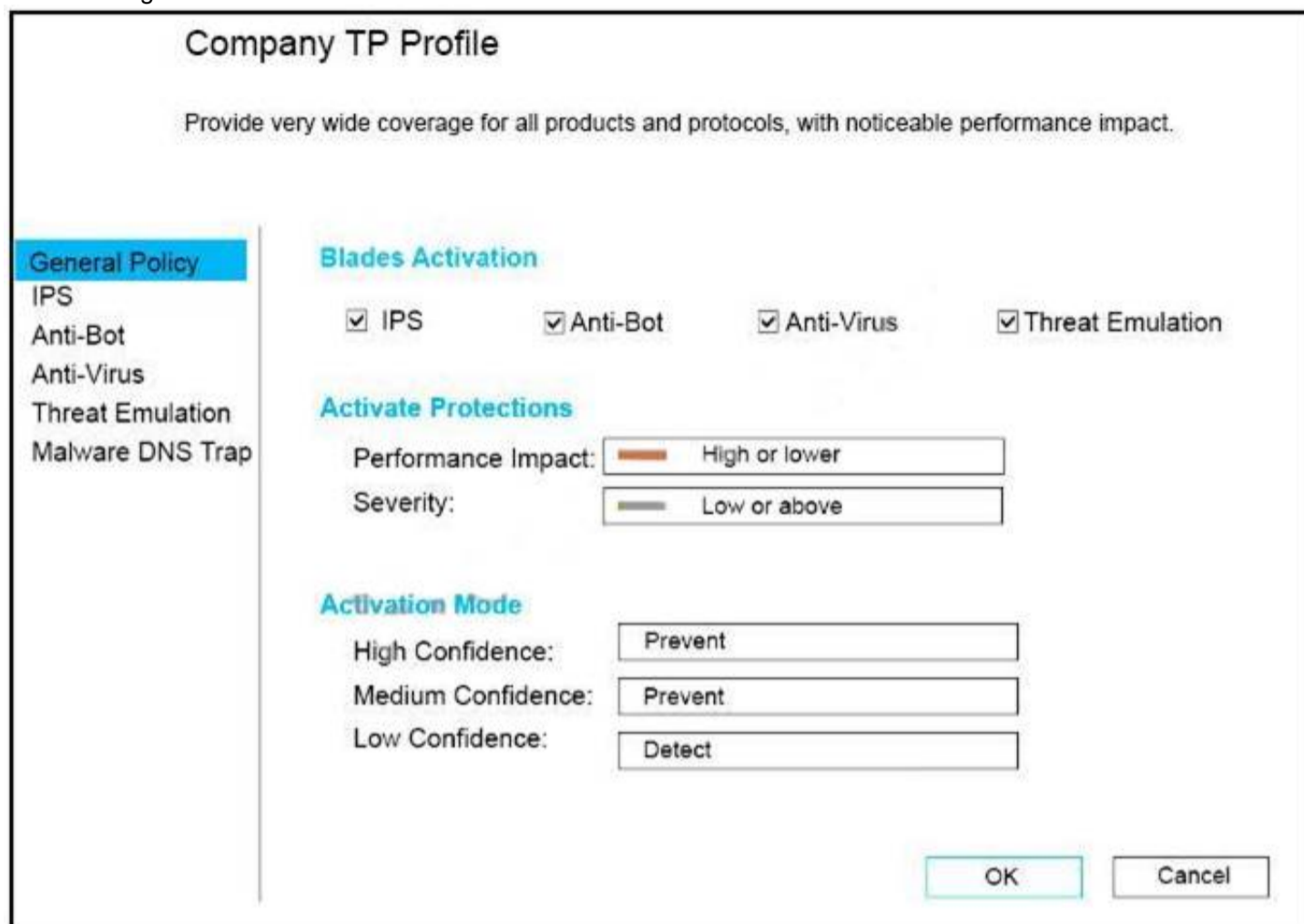
Which of the following is NOT an option to calculate the traffic direction?

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

Answer: D

NEW QUESTION 398

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.



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 400

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 402

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 406

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 411

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 416

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 420

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 425

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 426

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 430

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 432

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

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

Answer: D

NEW QUESTION 434

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 439

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 442

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

156-215.81 Practice Exam Features:

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

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