



CheckPoint

Exam Questions 156-215.81

Check Point Certified Security Administrator R81

NEW QUESTION 1

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 2

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 3

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 4

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 5

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 6

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 7

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 8

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 9

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 10

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 10

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 14

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

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

Answer: B

Explanation:

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

NEW QUESTION 16

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

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

Answer: ACD

NEW QUESTION 21

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

- A. Upgrade the software version
- B. Open WebUI

- C. Open SSH
- D. Open service request with Check Point Technical Support

Answer: C

NEW QUESTION 22

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 25

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 28

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 30

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 33

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 37

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

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

Answer: A

Explanation:

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

NEW QUESTION 42

Tom has connected to the Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward. What will happen to the changes already made?

- A. Tom will have to reboot his SmartConsole computer, clear the cache, and restore changes.
- B. Tom will have to reboot his SmartConsole computer, and access the Management cache store on that computer, which is only accessible after a reboot.
- C. Tom's changes will be lost since he lost connectivity and he will have to start again.
- D. Tom's changes will have been stored on the Management when he reconnects and he will not lose any of his work.

Answer: D

NEW QUESTION 44

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 49

Stateful Inspection compiles and registers connections where?

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

Answer: C

NEW QUESTION 52

A network administrator has informed you that they have identified a malicious host on the network, and instructed you to block it. Corporate policy dictates that firewall policy changes cannot be made at this time. What tool can you use to block this traffic?

- A. Anti-Bot protection
- B. Anti-Malware protection
- C. Policy-based routing
- D. Suspicious Activity Monitoring (SAM) rules

Answer: D

Explanation:

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

NEW QUESTION 56

SmartEvent does NOT use which of the following procedures to identify events:

- A. Matching a log against each event definition
- B. Create an event candidate
- C. Matching a log against local exclusions
- D. Matching a log against global exclusions

Answer: C

NEW QUESTION 59

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 61

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

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

Answer: C

NEW QUESTION 65

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 68

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 73

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 74

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 76

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 78

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 79

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 83

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 84

Which of the following is considered a "Subscription Blade", requiring renewal every 1-3 years?

- A. IPS blade
- B. IPSEC VPN Blade
- C. Identity Awareness Blade
- D. Firewall Blade

Answer: A

NEW QUESTION 87

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 89

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 94

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 97

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 100

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 103

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

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

Answer: B

NEW QUESTION 106

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 108

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 109

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

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

Answer: D

Explanation:

Stateful Inspection, the packet is intercepted at the network layer, but then the INSPECT Engine takes over.

It extracts state-related information required for the security decision from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts.

NEW QUESTION 111

In SmartConsole, on which tab are Permissions and Administrators defined?

- A. Manage and Settings
- B. Logs and Monitor
- C. Security Policies
- D. Gateways and Servers

Answer: A

NEW QUESTION 114

Fill in the blank: An LDAP server holds one or more _____.

- A. Server Units
- B. Administrator Units
- C. Account Units
- D. Account Servers

Answer: C

NEW QUESTION 118

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 121

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

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

Answer: B

NEW QUESTION 123

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 125

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

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

Answer: C

Explanation:

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

NEW QUESTION 130

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 131

Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 132

Which of the following situations would not require a new license to be generated and installed?

- A. The Security Gateway is upgraded.
- B. The existing license expires.

- C. The license is upgraded.
- D. The IP address of the Security Management or Security Gateway has changed.

Answer: A

NEW QUESTION 137

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 142

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 144

When an encrypted packet is decrypted, where does this happen?

- A. Security policy
- B. Inbound chain
- C. Outbound chain
- D. Decryption is not supported

Answer: A

NEW QUESTION 147

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 148

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 149

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 150

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 155

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 156

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 157

A Check Point Software license consists of two components, the Software Blade and the Software Container. There are _____ types of Software Containers: _____.

- A. Two; Security Management and Endpoint Security
- B. Two; Endpoint Security and Security Gateway
- C. Three; Security Management, Security Gateway, and Endpoint Security
- D. Three; Security Gateway, Endpoint Security, and Gateway Management

Answer: C

Explanation:

There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security. Ref: <https://downloads.checkpoint.com/dc/download.htm?ID=11608>

NEW QUESTION 158

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 159

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 160

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 163

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 167

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 168

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 169

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 174

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 175

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 177

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 182

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 186

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 189

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 191

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

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

Answer: D

Explanation:

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

NEW QUESTION 196

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 198

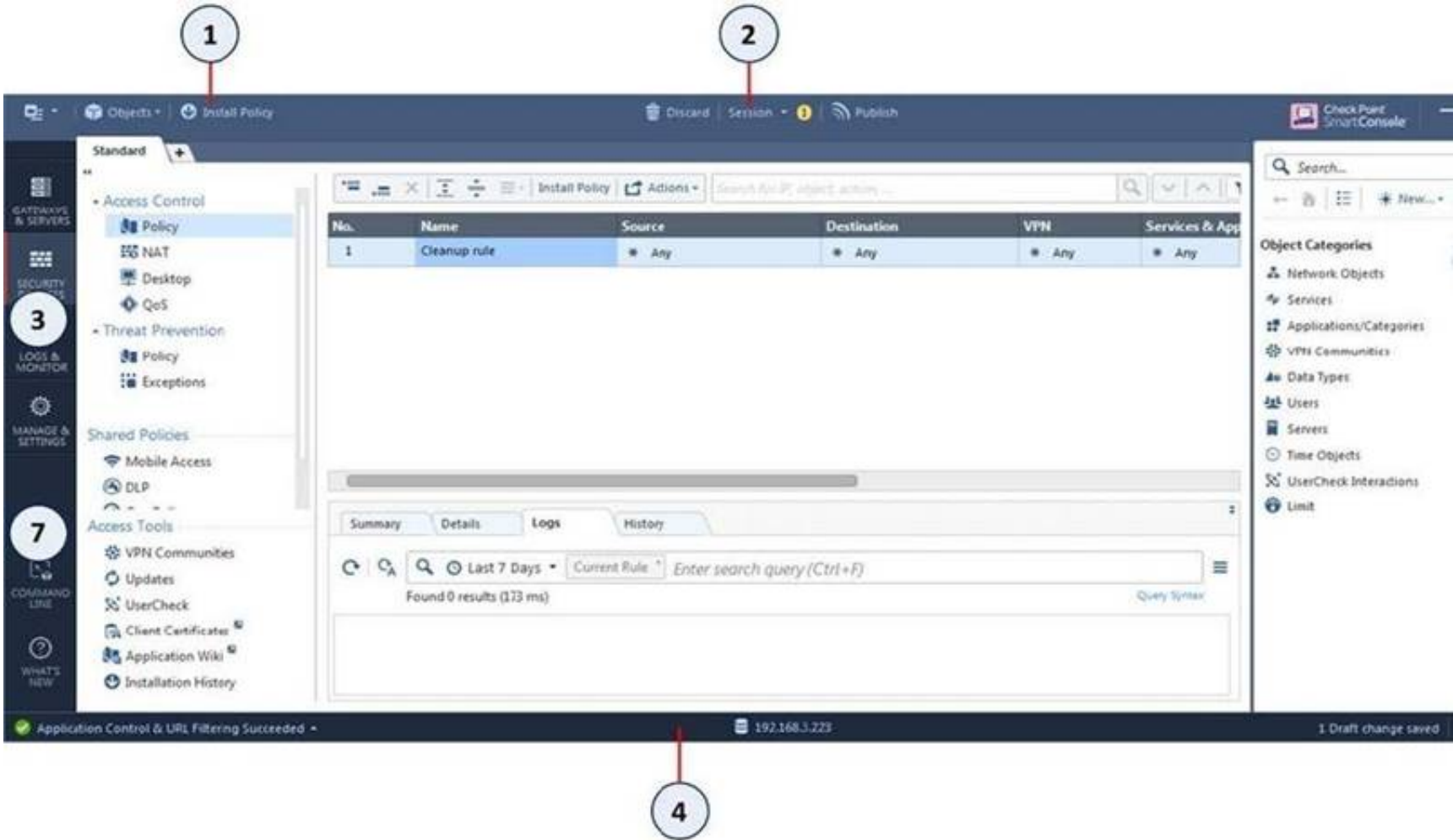
Which of the following is NOT a valid application navigation tab in the R80 SmartConsole?

- 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 200

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 204

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

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

Answer: C

Explanation:

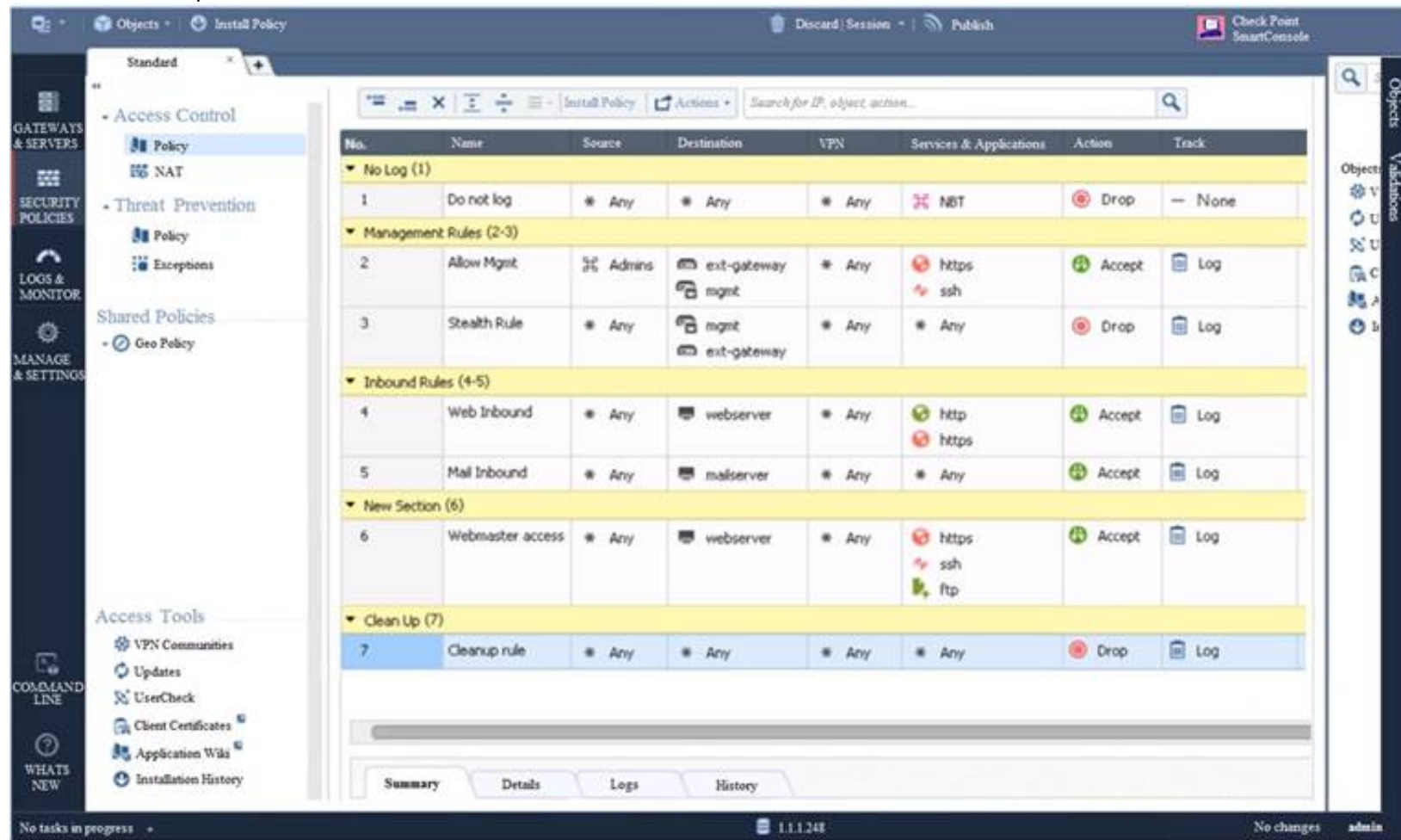
<https://community.checkpoint.com/t5/Check-Point-for-Beginners-2-0/Part-1-The-Architecture/ba-p/88043> Security Gateway (SG) is usually deployed on the perimeter to control and secure traffic with Firewall and Threat Prevention capabilities.

Security Management Server (SMS) defines and controls security policies on the Gateways. It can also be used to as a log server with built-in system of log indexing (SmartLog) and event correlation (SmartEvent – a SIEM-like solution for Check Point products). Usually, SMS is the main element of central management with multiple Security Gateways in operation. Nevertheless, you need an SMS even if your security system has a single gateway only.

SmartConsole is a GUI administration tool to connect to SMS. Through this tool, a security administrator is able to prepare and apply security policies to the Security Gateways.

NEW QUESTION 208

Examine the sample Rule Base.



No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	* Any	* Any	* Any	NBT	Drop	None
Management Rules (2-3)							
2	Allow Mgmt	admins	ext-gateway	* Any	https, ssh	Accept	Log
3	Stealth Rule	* Any	mgmt, ext-gateway	* Any	* Any	Drop	Log
Inbound Rules (4-5)							
4	Web Inbound	* Any	webserver	* Any	http, https	Accept	Log
5	Mail Inbound	* Any	mailserver	* Any	* Any	Accept	Log
New Section (6)							
6	Webmaster access	* Any	webserver	* Any	https, ssh, ftp	Accept	Log
Clean Up (7)							
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log

What will be the result of a verification of the policy from SmartConsole?

- A. No errors or Warnings
- B. Verification Error
- C. Empty Source-List in Rule 5 (Mail Inbound)
- D. Verification Error
- E. Rule 4 (Web Inbound) hides Rule 6 (Webmaster access)
- F. Verification Error
- G. Rule 7 (Clean-Up Rule) hides Implicit Clean-up Rule

Answer: C

NEW QUESTION 211

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 214

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 215

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

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

Answer: A

NEW QUESTION 217

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

Communication (SIC)?

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

Answer: A

Explanation:

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

NEW QUESTION 221

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 224

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 227

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

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

Answer: A

NEW QUESTION 230

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 233

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 235

What are the steps to configure the HTTPS Inspection Policy?

- A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
- B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
- C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
- D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: C

NEW QUESTION 239

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 241

.....

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](#)