

CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81



NEW QUESTION 1

- (Exam Topic 1)

SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's machine via the web browser. What are the two modes of SNX?

- A. Application and Client Service
- B. Network and Application
- C. Network and Layers
- D. Virtual Adapter and Mobile App

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

How can SmartView application accessed?

- A. `http://<Security Management IP Address>/smartview`
- B. `http://<Security Management IP Address>:4434/smartview/`
- C. `https://<Security Management IP Address>/smartview/`
- D. `https://<Security Management host name>:4434/smartview/`

Answer: C

NEW QUESTION 3

- (Exam Topic 1)

fwssd is a child process of which of the following Check Point daemons?

- A. fwd
- B. cpwd
- C. fwm
- D. cpd

Answer: A

NEW QUESTION 4

- (Exam Topic 1)

What is true about the IPS-Blade?

- A. In R81, IPS is managed by the Threat Prevention Policy
- B. In R81, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
- C. In R81, IPS Exceptions cannot be attached to "all rules"
- D. In R81, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 5

- (Exam Topic 1)

In order to get info about assignment (FW, SND) of all CPUs in your SGW, what is the most accurate CLI command?

- A. `fw ctl sdstat`
- B. `fw ctl affinity -l -a -r -v`
- C. `fw ctl multik stat`
- D. `cpinfo`

Answer: B

NEW QUESTION 6

- (Exam Topic 1)

Which command can you use to verify the number of active concurrent connections?

- A. `fw conn all`
- B. `fw ctl pstat`
- C. `show all connections`
- D. `show connections`

Answer: B

NEW QUESTION 7

- (Exam Topic 1)

The Security Gateway is installed on GAIA R81. The default port for the Web User Interface is _____.

- A. TCP 18211
- B. TCP 257
- C. TCP 4433
- D. TCP 443

Answer: D

NEW QUESTION 8

- (Exam Topic 1)

On R81.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

- A. 18210
- B. 18184
- C. 257
- D. 18191

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

What Factor preclude Secure XL Templating?

- A. Source Port Ranges/Encrypted Connections
- B. IPS
- C. ClusterXL in load sharing Mode
- D. CoreXL

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated management console. CPM allows the GUI client and management server to communicate via web services using _____.

- A. TCP port 19009
- B. TCP Port 18190
- C. TCP Port 18191
- D. TCP Port 18209

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Advanced Security Checkups can be easily conducted within:

- A. Reports
- B. Advanced
- C. Checkups
- D. Views
- E. Summary

Answer: A

NEW QUESTION 14

- (Exam Topic 1)

Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

- A. logd
- B. fwd
- C. fwm
- D. cpd

Answer: B

NEW QUESTION 16

- (Exam Topic 1)

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 21

- (Exam Topic 1)

Tom has been tasked to install Check Point R81 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

- A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
- B. One machine
- C. Two machines
- D. Three machines

Answer: C

Explanation:

One for Security Management Server and the other one for the Security Gateway.

NEW QUESTION 26

- (Exam Topic 1)

In R81, how do you manage your Mobile Access Policy?

- A. Through the Unified Policy
- B. Through the Mobile Console
- C. From SmartDashboard
- D. From the Dedicated Mobility Tab

Answer: A

NEW QUESTION 29

- (Exam Topic 1)

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 33

- (Exam Topic 1)

What is not a component of Check Point SandBlast?

- A. Threat Emulation
- B. Threat Simulator
- C. Threat Extraction
- D. Threat Cloud

Answer: B

NEW QUESTION 38

- (Exam Topic 1)

Which command lists all tables in Gaia?

- A. fw tab -t
- B. fw tab -list
- C. fw-tab -s
- D. fw tab -1

Answer: C

NEW QUESTION 42

- (Exam Topic 1)

Which of the following type of authentication on Mobile Access can NOT be used as the first authentication method?

- A. Dynamic ID
- B. RADIUS
- C. Username and Password
- D. Certificate

Answer: A

NEW QUESTION 44

- (Exam Topic 1)

Which two of these Check Point Protocols are used by SmartEvent Processes?

- A. ELA and CPD
- B. FWD and LEA
- C. FWD and CPLOG
- D. ELA and CPLOG

Answer: D

NEW QUESTION 47

- (Exam Topic 1)

How many images are included with Check Point TE appliance in Recommended Mode?

- A. 2(OS) images
- B. images are chosen by administrator during installation
- C. as many as licensed for
- D. the most new image

Answer: A

NEW QUESTION 48

- (Exam Topic 1)

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the "mgmt_cli" command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia's secure shell(clish)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 49

- (Exam Topic 1)

Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

- A. 50%
- B. 75%
- C. 80%
- D. 15%

Answer: D

NEW QUESTION 52

- (Exam Topic 1)

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 56

- (Exam Topic 1)

Which packet info is ignored with Session Rate Acceleration?

- A. source port ranges
- B. source ip
- C. source port
- D. same info from Packet Acceleration is used

Answer: B

NEW QUESTION 61

- (Exam Topic 1)

What command verifies that the API server is responding?

- A. api stat
- B. api status
- C. show api_status
- D. app_get_status

Answer: B

NEW QUESTION 62

- (Exam Topic 2)

Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

- A. cphaprob stat
- B. cphaprob -a if
- C. cphaprob -l list
- D. cphaprob all show stat

Answer:

D

NEW QUESTION 66

- (Exam Topic 2)

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 67

- (Exam Topic 2)

Which statements below are CORRECT regarding Threat Prevention profiles in SmartDashboard?

- A. You can assign only one profile per gateway and a profile can be assigned to one rule Only.
- B. You can assign multiple profiles per gateway and a profile can be assigned to one rule only.
- C. You can assign multiple profiles per gateway and a profile can be assigned to one or more rules.
- D. You can assign only one profile per gateway and a profile can be assigned to one or more rules.

Answer: C

NEW QUESTION 68

- (Exam Topic 2)

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 72

- (Exam Topic 2)

SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

- A. This statement is true because SecureXL does improve all traffic.
- B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
- C. This statement is true because SecureXL does improve this traffic.
- D. This statement is false because encrypted traffic cannot be inspected.

Answer: C

Explanation:

SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

NEW QUESTION 74

- (Exam Topic 2)

Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

- A. cpwd
- B. fwd
- C. cpd
- D. fwm

Answer: D

Explanation:

Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that require direct GUI access, such as SmartEvent, It provides the following:

- GUI Client communication
- Database manipulation
- Policy Compilation
- Management HA sync

NEW QUESTION 76

- (Exam Topic 2)

What information is NOT collected from a Security Gateway in a Cpinfo?

- A. Firewall logs
- B. Configuration and database files

- C. System message logs
- D. OS and network statistics

Answer: A

NEW QUESTION 78

- (Exam Topic 2)

You have existing dbedit scripts from R77. Can you use them with R81.10?

- A. dbedit is not supported in R81.10
- B. dbedit is fully supported in R81.10
- C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
- D. dbedit scripts are being replaced by mgmt_cli in R81.10

Answer: D

NEW QUESTION 81

- (Exam Topic 2)

Which encryption algorithm is the least secured?

- A. AES-128
- B. AES-256
- C. DES
- D. 3DES

Answer: C

NEW QUESTION 82

- (Exam Topic 2)

Which command shows the current connections distributed by CoreXL FW instances?

- A. fw ctl multik stat
- B. fw ctl affinity -l
- C. fw ctl instances -v
- D. fw ctl iflist

Answer: A

NEW QUESTION 84

- (Exam Topic 2)

Which Check Point daemon monitors the other daemons?

- A. fwm
- B. cpd
- C. cpwd
- D. fwssd

Answer: C

NEW QUESTION 87

- (Exam Topic 2)

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 90

- (Exam Topic 2)

What command can you use to have cpinfo display all installed hotfixes?

- A. cpinfo -hf
- B. cpinfo -y all
- C. cpinfo -get hf
- D. cpinfo installed_jumbo

Answer: B

NEW QUESTION 95

- (Exam Topic 2)

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

Explanation:

Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:

- Matching a Log Against Global Exclusions
- Matching a Log Against Each Event Definition
- Creating an Event Candidate
- When a Candidate Becomes an Event References:

NEW QUESTION 98

- (Exam Topic 2)

What is mandatory for ClusterXL to work properly?

- A. The number of cores must be the same on every participating cluster node
- B. The Magic MAC number must be unique per cluster node
- C. The Sync interface must not have an IP address configured
- D. If you have “Non-monitored Private” interfaces, the number of those interfaces must be the same on all cluster members

Answer: B

NEW QUESTION 99

- (Exam Topic 2)

To add a file to the Threat Prevention Whitelist, what two items are needed?

- A. File name and Gateway
- B. Object Name and MD5 signature
- C. MD5 signature and Gateway
- D. IP address of Management Server and Gateway

Answer: B

NEW QUESTION 100

- (Exam Topic 2)

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 105

- (Exam Topic 2)

Which one of the following is true about Capsule Connect?

- A. It is a full layer 3 VPN client
- B. It offers full enterprise mobility management
- C. It is supported only on iOS phones and Windows PCs
- D. It does not support all VPN authentication methods

Answer: A

NEW QUESTION 107

- (Exam Topic 2)

What is the command to check the status of the SmartEvent Correlation Unit?

- A. fw ctl get int cpsead_stat
- B. cpstat cpsead
- C. fw ctl stat cpsemd
- D. cp_conf get_stat cpsemd

Answer: B

NEW QUESTION 108

- (Exam Topic 2)

Which statement is true about ClusterXL?

- A. Supports Dynamic Routing (Unicast and Multicast)
- B. Supports Dynamic Routing (Unicast Only)
- C. Supports Dynamic Routing (Multicast Only)

D. Does not support Dynamic Routing

Answer: A

NEW QUESTION 113

- (Exam Topic 2)

Which of the following links will take you to the SmartView web application?

- A. <https://<Security Management Server host name>/smartviewweb/>
- B. <https://<Security Management Server IP Address>/smartview/>
- C. <https://<Security Management Server host name>smartviewweb>
- D. <https://<Security Management Server IP Address>/smartview>

Answer: B

NEW QUESTION 116

- (Exam Topic 2)

When installing a dedicated R81 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 20GB
- D. At least 20GB

Answer: D

NEW QUESTION 119

- (Exam Topic 2)

You want to store the GAIA configuration in a file for later reference. What command should you use?

- A. write mem <filename>
- B. show config -f <filename>
- C. save config -o <filename>
- D. save configuration <filename>

Answer: D

NEW QUESTION 124

- (Exam Topic 2)

Which web services protocol is used to communicate to the Check Point R81 Identity Awareness Web API?

- A. SOAP
- B. REST
- C. XLANG
- D. XML-RPC

Answer: B

Explanation:

The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

NEW QUESTION 129

- (Exam Topic 2)

Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R81.10 SmartConsole application?

- A. IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.
- B. Firewall, IPS, Threat Emulation, Application Control.
- C. IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.
- D. Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.

Answer: C

NEW QUESTION 132

- (Exam Topic 2)

The following command is used to verify the CPUSE version:

- A. HostName:0>show installer status build
- B. [Expert@HostName:0]#show installer status
- C. [Expert@HostName:0]#show installer status build
- D. HostName:0>show installer build

Answer: A

NEW QUESTION 134

- (Exam Topic 3)

Which statement is most correct regarding about “CoreXL Dynamic Dispatcher”?

- A. The CoreXL FW instanxces assignment mechanism is based on Source MAC addresses, Destination MAC addresses
- B. The CoreXL FW instances assignment mechanism is based on the utilization of CPU cores
- C. The CoreXL FW instances assignment mechanism is based on IP Protocol type
- D. The CoreXI FW instances assignment mechanism is based on Source IP addresses, Destination IP addresses, and the IP ‘Protocol’ type

Answer: B

NEW QUESTION 136

- (Exam Topic 3)

GAiA Software update packages can be imported and installed offline in situation where:

- A. Security Gateway with GAiA does NOT have SFTP access to Internet
- B. Security Gateway with GAiA does NOT have access to Internet.
- C. Security Gateway with GAiA does NOT have SSH access to Internet.
- D. The desired CPUSE package is ONLY available in the Check Point CLOUD.

Answer: B

NEW QUESTION 137

- (Exam Topic 3)

Check Point APIs allow system engineers and developers to make changes to their organization’s security policy with CLI tools and Web Services for all the following except:

- A. Create new dashboards to manage 3rd party task
- B. Create products that use and enhance 3rd party solutions
- C. Execute automated scripts to perform common tasks
- D. Create products that use and enhance the Check Point Solution

Answer: A

Explanation:

Check Point APIs let system administrators and developers make changes to the security policy with CLI tools and web-services. You can use an API to:

- Use an automated script to perform common tasks
- Integrate Check Point products with 3rd party solutions
- Create products that use and enhance the Check Point solution References:

NEW QUESTION 141

- (Exam Topic 3)

Office mode means that:

- A. SecurID client assigns a routable MAC addres
- B. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.
- C. Users authenticate with an Internet browser and use secure HTTPS connection.
- D. Local ISP (Internet service Provider) assigns a non-routable IP address to the remote user.
- E. Allows a security gateway to assign a remote client an IP addres
- F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

NEW QUESTION 144

- (Exam Topic 3)

What command lists all interfaces using Multi-Queue?

- A. cpmq get
- B. show interface all
- C. cpmq set
- D. show multiqueue all

Answer: A

NEW QUESTION 148

- (Exam Topic 3)

What is not a purpose of the deployment of Check Point API?

- A. Execute an automated script to perform common tasks
- B. Create a customized GUI Client for manipulating the objects database
- C. Create products that use and enhance the Check Point solution
- D. Integrate Check Point products with 3rd party solution

Answer: B

NEW QUESTION 151

- (Exam Topic 3)

What kind of information would you expect to see using the sim affinity command?

- A. The VMACs used in a Security Gateway cluster
- B. The involved firewall kernel modules in inbound and outbound packet chain
- C. Overview over SecureXL templated connections
- D. Network interfaces and core distribution used for CoreXL

Answer: D

NEW QUESTION 154

- (Exam Topic 3)

What is UserCheck?

- A. Messaging tool used 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

NEW QUESTION 156

- (Exam Topic 3)

What CLI command compiles and installs a Security Policy on the target's Security Gateways?

- A. fwm compile
- B. fwm load
- C. fwm fetch
- D. fwm install

Answer: B

NEW QUESTION 159

- (Exam Topic 3)

Which blades and or features are not supported in R81?

- A. SmartEvent Maps
- B. SmartEvent
- C. Identity Awareness
- D. SmartConsole Toolbars

Answer: A

NEW QUESTION 161

- (Exam Topic 3)

In what way are SSL VPN and IPSec VPN different?

- A. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
- B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
- C. IPSec VPN does not support two factor authentication, SSL VPN does support this
- D. IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only.

Answer: D

NEW QUESTION 164

- (Exam Topic 3)

You want to verify if your management server is ready to upgrade to R81.10. What tool could you use in this process?

- A. migrate export
- B. upgrade_tools verify
- C. pre_upgrade_verifier
- D. migrate import

Answer: C

NEW QUESTION 165

- (Exam Topic 3)

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 168

- (Exam Topic 3)

In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Stateful Mode configuration, chain modules marked with _____ will not apply.

- A. ffff
- B. 1
- C. 3
- D. 2

Answer: D

NEW QUESTION 169

- (Exam Topic 3)

When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

- A. ThreatCloud is a database-related application which is located on-premise to preserve privacy of company-related data
- B. ThreatCloud is a collaboration platform for all the CheckPoint customers to form a virtual cloud consisting of a combination of all on-premise private cloud environments
- C. ThreatCloud is a collaboration platform for Check Point customers to benefit from VMWare ESXi infrastructure which supports the Threat Emulation Appliances as virtual machines in the EMC Cloud
- D. ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary

Answer: D

NEW QUESTION 172

- (Exam Topic 3)

For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

- A. 20 minutes
- B. 15 minutes
- C. Admin account cannot be unlocked automatically
- D. 30 minutes at least

Answer: D

NEW QUESTION 174

- (Exam Topic 3)

What must you do first if “fwm sic_reset” could not be completed?

- A. Cpstop then find keyword “certificate” in objects_5_0.C and delete the section
- B. Reinitialize SIC on the security gateway then run “fw unloadlocal”
- C. Reset SIC from Smart Dashboard
- D. Change internal CA via cpconfig

Answer: D

NEW QUESTION 176

- (Exam Topic 3)

What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?

- A. 4 Interfaces – an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.
- B. 3 Interfaces – an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
- C. 1 Interface – an interface leading to the organization and the Internet, and configure for synchronization.
- D. 2 Interfaces – a data interface leading to the organization and the Internet, a second interface for synchronization.

Answer: B

NEW QUESTION 180

- (Exam Topic 3)

What is the most ideal Synchronization Status for Security Management Server High Availability deployment?

- A. Lagging
- B. Synchronized
- C. Never been synchronized
- D. Collision

Answer: B

NEW QUESTION 185

- (Exam Topic 3)

What is the valid range for VRID value in VRRP configuration?

- A. A.-1 - 254B.1 - 255C.0 - 254D.0 - 255

Answer: B

Explanation:

Virtual Router ID - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255.

NEW QUESTION 189

- (Exam Topic 3)

With SecureXL enabled, accelerated packets will pass through the following:

- A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
- B. Network Interface Card, Check Point Firewall Kernel, and the Acceleration Device
- C. Network Interface Card and the Acceleration Device
- D. Network Interface Card, OSI Network Layer, and the Acceleration Device

Answer: C

NEW QUESTION 193

- (Exam Topic 3)

When attempting to start a VPN tunnel, in the logs the error “no proposal chosen” is seen numerous times. No other VPN-related entries are present. Which phase of the VPN negotiations has failed?

- A. IKE Phase 1
- B. IPSEC Phase 2
- C. IPSEC Phase 1
- D. IKE Phase 2

Answer: A

NEW QUESTION 198

- (Exam Topic 4)

What are the minimum open server hardware requirements for a Security Management Server/Standalone in R81?

- A. 2 CPU cores, 4GB of RAM and 15GB of disk space
- B. 8 CPU cores, 16GB of RAM and 500 GB of disk space
- C. 4 CPU cores, 8GB of RAM and 500GB of disk space
- D. 8 CPU cores, 32GB of RAM and 1 TB of disk space

Answer: C

NEW QUESTION 203

- (Exam Topic 4)

How would you enable VMAc Mode in ClusterXL?

- A. Cluster Object -> Edit -> ClusterXL and VRRP -> Use Virtual MAC
- B. fw ctl set int vmac_mode 1
- C. cphaconf vmac_mode set 1
- D. Cluster Object -> Edit -> Cluster Members -> Edit -> Use Virtual MAC

Answer: A

Explanation:

Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk50840

NEW QUESTION 205

- (Exam Topic 4)

When Configuring Endpoint Compliance Settings for Applications and Gateways within Mobile Access, which of the three approaches will allow you to configure individual policies for each application?

- A. Basic Approach
- B. Strong Approach
- C. Very Advanced Approach
- D. Medium Approach

Answer: C

NEW QUESTION 208

- (Exam Topic 4)

If SecureXL is disabled which path is used to process traffic?

- A. Passive path
- B. Medium path
- C. Firewall path
- D. Accelerated path

Answer: C

NEW QUESTION 212

- (Exam Topic 4)

After finishing installation admin John likes to use top command in expert mode. John has to set the expert-password and was able to use top command. A week later John has to use the top command again, He detected that the expert password is no longer valid. What is the most probable reason for this behavior?

- A. "write memory" was not issued on clish
- B. changes are only possible via SmartConsole
- C. "save config" was not issued in expert mode
- D. "save config" was not issued on clish

Answer: D

NEW QUESTION 213

- (Exam Topic 4)

A user complains that some Internet resources are not available. The Administrator is having issues seeing it packets are being dropped at the firewall (not seeing drops in logs). What is the solution to troubleshoot the issue?

- A. run fw unloadlocal" on the relevant gateway and check the ping again
- B. run "cpstop" on the relevant gateway and check the ping again
- C. run "fw log" on the relevant gateway
- D. run "fw ctl zdebug drop" on the relevant gateway

Answer: D

NEW QUESTION 215

- (Exam Topic 4)

There are multiple types of licenses for the various VPN components and types. License type related to management and functioning of Remote Access VPNs are - which of the following license requirement statement is NOT true:

- A. MobileAccessLicense ° This license is required on the Security Gateway for the following Remote Access solutions
- B. EndpointPolicyManagementLicense ° The Endpoint Security Suite includes blades other than the Remote Access VPN, hence this license is required to manage the suite
- C. EndpointContainerLicense ° The Endpoint Software Blade Licenses does not require an Endpoint Container License as the base
- D. IPSecVPNLicense • This license is installed on the VPN Gateway and is a basic requirement for a Remote Access VPN solution

Answer: C

NEW QUESTION 217

- (Exam Topic 4)

Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

- A. Formal; corporate
- B. Local; formal
- C. Local; central
- D. Central; local

Answer: D

NEW QUESTION 220

- (Exam Topic 4)

The back end database for Check Point R81 Management uses:

- A. DBMS
- B. MongoDB
- C. PostgreSQL
- D. MySQL

Answer: C

NEW QUESTION 224

- (Exam Topic 4)

D18912E1457D5D1DDCBBD40AB3BF70D5D

The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule based and checked for viruses. But it is not accelerated. What is the most likely reason that the traffic is not accelerated?

- A. The connection is destined for a server within the network
- B. The connection required a Security server
- C. The packet is the second in an established TCP connection
- D. The packets are not multicast

Answer: B

NEW QUESTION 225

- (Exam Topic 4)

Which feature is NOT provided by all Check Point Mobile Access solutions?

- A. Support for IPv6
- B. Granular access control
- C. Strong user authentication
- D. Secure connectivity

Answer: A

Explanation:

Types of Solutions

All of Check Point's Remote Access solutions provide:

NEW QUESTION 229

- (Exam Topic 4)

What are types of Check Point APIs available currently as part of R81.10 code?

- A. Security Gateway API Management API, Threat Prevention API and Identity Awareness Web Services API
- B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
- C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
- D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

NEW QUESTION 234

- (Exam Topic 4)

Which utility allows you to configure the DHCP service on Gaia from the command line?

- A. ifconfig
- B. dhcp_ofg
- C. sysconfig
- D. cpconfig

Answer: C

NEW QUESTION 237

- (Exam Topic 4)

What a valid SecureXL paths in R81.10?

- A. F2F (Slow path). Templated Pat
- B. PQX and F2V
- C. F2F (Slow path). PXL, QXL and F2V
- D. F2F (Slow path), Accelerated Path, PQX and F2V
- E. F2F (Slow path), Accelerated Path, Medium Path and F2V

Answer: D

NEW QUESTION 240

- (Exam Topic 4)

You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the tight protections in place. Check Point has been selected for the security vendor.

Which Check Point product protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

- A. IPS AND Application Control
- B. IPS, anti-virus and anti-bot
- C. IPS, anti-virus and e-mail security
- D. SandBlast

Answer: D

NEW QUESTION 242

- (Exam Topic 4)

After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?

- A. You will find it in the home directory of your usef account (e.
- B. /home/admirV)
- C. You can locate the file via SmartConsole > Command Line.
- D. You have to launch the WebUI and go to "Config" -> "Export Conflg File" and specify the destination directory of your local tile system
- E. You cannot locate the file in the file system sine© Clish does not have any access to the bash fie system

Answer: B

NEW QUESTION 246

- (Exam Topic 4)

After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?

- A. You will find it in the home directory of your user account (e.
- B. /home/admin/)

- C. You can locate the file via SmartConsole > Command Line.
- D. You have to launch the WebUI and go to "Config" -> "Export Config File" and specify the destination directory of your local file system.
- E. You cannot locate the file in the file system since Clish does not have any access to the bash file system

Answer: A

NEW QUESTION 250

- (Exam Topic 4)

What command is used to manually failover a Multi-Version Cluster during the upgrade?

- A. clusterXL_admin down in Expert Mode
- B. clusterXL_admin down in Clish
- C. set cluster member state down in Clish
- D. set cluster down in Expert Mode

Answer: B

NEW QUESTION 255

- (Exam Topic 4)

John detected high load on sync interface. Which is most recommended solution?

- A. For FTP connections – do not sync
- B. Add a second interface to handle sync traffic
- C. For short connections like http service – do not sync
- D. For short connections like icmp service – delay sync for 2 seconds

Answer: A

NEW QUESTION 259

- (Exam Topic 4)

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 if the Track option is set to “None”?

- A. No, it will work independentl
- B. Hit Count will be shown only for rules Track option 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 261

- (Exam Topic 4)

You had setup the VPN Community VPN-Stores'with 3 gateways. There are some issues with one remote gateway(1.1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways

- A. action:"Key Install" AND 1.1.1.1 AND Main Mode
- B. action:"Key Install- AND 1.1.1.1 ANDQuick Mode
- C. Blade:"VPN" AND VPN-Stores AND Main Mode
- D. Blade:"VPN" AND VPN-Stores AND Quick Mode

Answer: C

NEW QUESTION 266

- (Exam Topic 4)

Packet acceleration (SecureXL) identities connections by several attributes. Which of the attributes is NOT used for identifying connection?

- A. Source Port
- B. TCP Acknowledgment Number
- C. Source Address
- D. Destination Address

Answer: B

NEW QUESTION 270

- (Exam Topic 4)

What is a possible command to delete all of the SSH connections of a gateway?

- A. fw sam -l dport 22
- B. fw ctl conntab -x -dpott=22
- C. fw tab -t connections -x -e 00000016
- D. fwaccel dos config set dport ssh

Answer: A

NEW QUESTION 271

- (Exam Topic 4)

In which VPN community is a satellite VPN gateway not allowed to create a VPN tunnel with another satellite VPN gateway?

- A. Pentagon
- B. Combined
- C. Meshed
- D. Star

Answer: D

NEW QUESTION 276

- (Exam Topic 4)

What solution is Multi-queue intended to provide?

- A. Improve the efficiency of traffic handling by SecureXL SNDs
- B. Reduce the confusion for traffic capturing in FW Monitor
- C. Improve the efficiency of CoreXL Kernel Instances
- D. Reduce the performance of network interfaces

Answer: C

NEW QUESTION 278

- (Exam Topic 4)

Can Check Point and Third-party Gateways establish a certificate-based Site-to-Site VPN tunnel?

- A. Yes, but they need to have a mutually trusted certificate authority
- B. Yes, but they have to have a pre-shared secret key
- C. No, they cannot share certificate authorities
- D. No, Certificate based VPNs are only possible between Check Point devices

Answer: A

NEW QUESTION 279

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 281

- (Exam Topic 4)

Which of the following is NOT an internal/native Check Point command?

- A. fwaccel on
- B. fw ct1 debug
- C. tcpdump
- D. cphaprob

Answer: C

NEW QUESTION 286

- (Exam Topic 4)

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

- A. Run cprestart from clish
- B. After upgrading the hardware, increase the number of kernel instances using cpconfig
- C. Administrator does not need to perform any tas
- D. Check Point will make use of the newly installed CPU and Cores
- E. Hyperthreading must be enabled in the bios to use CoreXL

Answer: B

NEW QUESTION 291

- (Exam Topic 4)

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track
No Log (1)							
1	Do not log	Any	Any	Any	NET	Drop	None
Management Rules (2-3)							
2	Allow Mgmt	Admins	ext-gateway mgmt	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	smtp pop-3 imap	Accept	Log
New Section (6)							
6	Webmaster access to servers	Any	webserver mailserver	Any	https ssh ftp	Accept	Log
Clean Up (7)							
7	Cleanup rule	Any	Any	Any	Any	Drop	Log

What can we infer about the recent changes made to the Rule Base?

- A. Rule 7 was created by the 'admin' administrator in the current session
- B. 8 changes have been made by administrators since the last policy installation
- C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator
- D. Rule 1 and object webserver are locked by another administrator

Answer: D

NEW QUESTION 293

- (Exam Topic 4)

What is the base level encryption key used by Capsule Docs?

- A. RSA 2048
- B. RSA 1024
- C. SHA-256
- D. AES

Answer: A

NEW QUESTION 297

- (Exam Topic 4)

According to out of the box SmartEvent policy, which blade will automatically be correlated into events?

- A. Firewall
- B. VPN
- C. IPS
- D. HTTPS

Answer: C

NEW QUESTION 299

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

- A. 18191
- B. 18190
- C. 8983
- D. 19009

Answer: D

NEW QUESTION 304

- (Exam Topic 4)

What should the admin do in case the Primary Management Server is temporary down?

- A. Use the VIP in SmartConsole you always reach the active Management Server.
- B. The Secondary will take over automatically Change the IP in SmartConsole to logon to the private IP of the Secondary Management Server.
- C. Run the 'promote_util' to activate the Secondary Management server
- D. Logon with SmartConsole to the Secondary Management Server and choose "Make Active" under Actions in the HA Management Menu

Answer: A

NEW QUESTION 305

- (Exam Topic 4)

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	* Any	* Any	* Any	NBT	Drop	None	Policy Targets
2	Management	Net_10.28.0.0	GW-R7730	* Any	https, ssh	Accept	Log	Policy Targets
3	Stealth	* Any	GW-R7730	* Any	* Any	Drop	Log	Policy Targets
4	DNS	Net_10.28.0.0	* Any	* Any	dns	Accept	Log	Policy Targets
5	Web	Net_10.28.0.0	* Any	* Any	http, https	Accept	Log	Policy Targets
6	DMZ Access	Net_10.28.0.0	DMZ_Net_192.0.2.0	* Any	ftp, AP-Defender	Accept	Log	Policy Targets
7	Cleanup rule	* Any	* Any	* Any	* Any	Drop	Log	Policy Targets

You are the administrator for ABC Corp. You have logged into your R81 Management server. You are making some changes in the Rule Base and notice that rule No.6 has a pencil icon next to it.

What does this mean?

- A. This rule N
- B. 6 has been marked for deletion in your Management session.
- C. This rule N
- D. 6 has been marked for deletion in another Management session.
- E. This rule N
- F. 6 has been marked for editing in your Management session.
- G. This rule N
- H. 6 has been marked for editing in another Management session.

Answer: C

NEW QUESTION 306

- (Exam Topic 4)

The WebUI offers several methods for downloading hotfixes via CPUSE except:

- A. Automatic
- B. Force override
- C. Manually
- D. Scheduled

Answer: B

NEW QUESTION 308

- (Exam Topic 4)

Which of the following is NOT supported by CPUSE?

- A. Automatic download of full installation and upgrade packages
- B. Automatic download of hotfixes
- C. Installation of private hotfixes
- D. Offline installations

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109

NEW QUESTION 309

- (Exam Topic 4)

If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

- A. Nothing - the proxy ARP is automatically handled in the R81 version
- B. Add the proxy ARP configurations in a file called /etc/conf/local.arp
- C. Add the proxy ARP configurations in a file called \$FWDIR/conf/local.arp
- D. Add the proxy ARP configurations in a file called \$CPDIR/conf/local.arp

Answer: D

NEW QUESTION 313

- (Exam Topic 4)

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.
- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server.

Answer: D

NEW QUESTION 317

- (Exam Topic 4)

When users connect to the Mobile Access portal they are unable to open File Shares. Which log file would you want to examine?

- A. cvpnd.elg
- B. httpd.elg
- C. vpnd.elg
- D. fw.elg

Answer: A

NEW QUESTION 318

- (Exam Topic 4)

Bob is asked by Alice to disable the SecureXL mechanism temporary for further diagnostic by their Check Point partner. Which of the following Check Point Command is true:

- A. fwaccel suspend
- B. fwaccel standby
- C. fwaccel off
- D. fwaccel templates

Answer: C

NEW QUESTION 322

- (Exam Topic 4)

John is using Management HA. Which Security Management Server should he use for making changes?

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

Answer: B

NEW QUESTION 323

- (Exam Topic 4)

What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?





- A. Use Multi-Domain Management Server.
- B. Choose different setting for log storage and SmartEvent db
- C. Install Management and SmartEvent on different machines.
- D. it is not possible.

Answer: C

NEW QUESTION 327

- (Exam Topic 4)

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

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

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

Answer: A

NEW QUESTION 330

- (Exam Topic 4)

Bob has finished to setup provisioning a secondary security management server. Now he wants to check if the provisioning has been correct. Which of the following Check Point command can be used to check if the security management server has been installed as a primary or a secondary security management server?

- A. cprod_util MgmtlsPrimary
- B. cprod_util FwlsSecondary
- C. cprod_util MgmtlsSecondary
- D. cprod_util FwlsPrimary

Answer: A

NEW QUESTION 333

- (Exam Topic 4)

By default, the R81 web API uses which content-type in its response?

- A. Java Script
- B. XML
- C. Text
- D. JSON

Answer: D

NEW QUESTION 334

- (Exam Topic 4)

Joey want to configure NTP on R81 Security Management Server. He decided to do this via WebUI. What is the correct address to access the Web UI for Gaia platform via browser?

- A. https://<Device_IP_Address>
- B. http://<Device_IP_Address>:443
- C. https://<Device_IP_Address>:10000
- D. https://<Device_IP_Address>:4434

Answer: A

NEW QUESTION 336

- (Exam Topic 4)

Which options are given on features, when editing a Role on Gaia Platform?

- A. Read/Write, Read Only
- B. Read/Write, Read Only, None
- C. Read/Write, None
- D. Read Only, None

Answer: B

NEW QUESTION 340

- (Exam Topic 4)

What is the benefit of Manual NAT over Automatic NAT?

- A. If you create a new Security Policy, the Manual NAT rules will be transferred to this new policy.
- B. There is no benefit since Automatic NAT has in any case higher priority over Manual NAT
- C. You have the full control about the priority of the NAT rules
- D. On IPSO and GAIA Gateways, it is handled in a stateful manner

Answer: C

NEW QUESTION 343

- (Exam Topic 4)

Besides fw monitor, what is another command that can be used to capture packets?

- A. arp
- B. traceroute
- C. tcpdump
- D. ping

Answer: C

NEW QUESTION 348

- (Exam Topic 4)

You want to gather data and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

- A. Check Point Capsule Cloud
- B. Sandblast Mobile Protect
- C. SecuRemote
- D. SmartEvent Client Info

Answer: B

Explanation:

SandBlast Mobile Protect is a lightweight app for iOS and Android™ that gathers data and helps analyze threats to devices in your environment.
<https://www.checkpoint.com/downloads/products/how-sandblast-mobile-works-solution-brief.pdf>

NEW QUESTION 349

- (Exam Topic 4)

Which one is not a valid Package Option In the Web GUI for CPUSE?

- A. Clean Install

- B. Export Package
- C. Upgrade
- D. Database Conversion to R81.10 only

Answer: B

NEW QUESTION 354

- (Exam Topic 4)

Which of the following is a task of the CPD process?

- A. Invoke and monitor critical processes and attempts to restart them if they fail
- B. Transfers messages between Firewall processes
- C. Log forwarding
- D. Responsible for processing most traffic on a security gateway

Answer: B

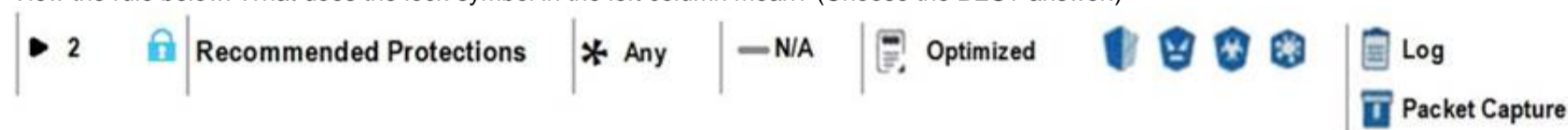
Explanation:

https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12496.htm

NEW QUESTION 355

- (Exam Topic 4)

View the rule below. What does the lock-symbol in the left column mean? (Choose the BEST answer.)



- A. The current administrator has read-only permissions to Threat Prevention Policy.
- B. Another user has locked the rule for editing.
- C. Configuration lock is present
- D. Click the lock symbol to gain read-write access.
- E. The current administrator is logged in as read-only because someone else is editing the policy.

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R81/CP_R81_SecMGMT/html_frameset.htm?topic=documents/R81/CP_

NEW QUESTION 360

- (Exam Topic 4)

You want to allow your Mobile Access Users to connect to an internal file share. Adding the Mobile Application 'File Share' to your Access Control Policy in the SmartConsole didn't work. You will be only allowed to select Services for the 'Service & Application' column. How to fix it?

- A. A Quantum Spark Appliance is selected as Installation Target for the policy packet.
- B. The Mobile Access Blade is not enabled for the Access Control Layer of the policy.
- C. The Mobile Access Policy Source under Gateway properties is set to Legacy Policy and not to Unified Access Policy.
- D. The Mobile Access Blade is not enabled under Gateway properties.

Answer: C

NEW QUESTION 362

- (Exam Topic 4)

What component of Management is used for indexing?

- A. DBSync
- B. API Server
- C. fwm
- D. SOLR

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_Multi-DomainSecurityManag

NEW QUESTION 364

- (Exam Topic 4)

You have enabled "Full 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. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R81 gateways.

Answer: A

NEW QUESTION 366

- (Exam Topic 4)

UserCheck objects in the Application Control and URL Filtering rules allow the gateway to communicate with the users. Which action is not supported in UserCheck objects?

- A. Ask
- B. Drop
- C. Inform
- D. Reject

Answer: D

NEW QUESTION 368

- (Exam Topic 4)

What destination versions are supported for a Multi-Version Cluster Upgrade?

- A. R81.40 and later
- B. R76 and later
- C. R70 and Later
- D. R81.10 and Later

Answer: D

NEW QUESTION 372

- (Exam Topic 4)

Which of the following is NOT an attribute of packet acceleration?

- A. Source address
- B. Protocol
- C. Destination port
- D. VLAN Tag

Answer: D

NEW QUESTION 374

- (Exam Topic 4)

The log server sends what to the Correlation Unit?

- A. Authentication requests
- B. CPML dbsync
- C. Logs
- D. Event Policy

Answer: C

NEW QUESTION 379

- (Exam Topic 4)

Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (EL-A) services.

- A. DASSERVICE
- B. FWD
- C. CPVIEWD
- D. CPD

Answer: A

NEW QUESTION 381

- (Exam Topic 4)

After verifying that API Server is not running, how can you start the API Server?

- A. Run command "set api start" in CLISH mode
- B. Run command "mgmt cli set api start" in Expert mode
- C. Run command "mgmt api start" in CLISH mode
- D. Run command "api start" in Expert mode

Answer: B

NEW QUESTION 386

- (Exam Topic 4)

Which command is used to add users to or from existing roles?

- A. Add rba user <User Name> roles <List>
- B. Add rba user <User Name>
- C. Add user <User Name> roles <List>
- D. Add user <User Name>

Answer: A

NEW QUESTION 387

- (Exam Topic 4)

Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?

- A. \$FWDIR/conf/client.scv
- B. \$CPDIR/conf/local.scv
- C. \$CPDIR/conf/client.svc
- D. \$FWDIR/conf/local.scv

Answer: D

Explanation:

https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG

NEW QUESTION 388

- (Exam Topic 4)

SmartEvent uses it's event policy to identify events. How can this be customized?

- A. By modifying the firewall rulebase
- B. By creating event candidates
- C. By matching logs against exclusions
- D. By matching logs against event rules

Answer: D

NEW QUESTION 393

- (Exam Topic 4)

Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

- A. To satellites through center only
- B. To center only
- C. To center and to other satellites through center
- D. To center, or through the center to other satellites, to Internet and other VPN targets

Answer: D

NEW QUESTION 394

- (Exam Topic 4)

Which of the following Central Deployment is NOT a limitation in R81.10 SmartConsole?

- A. Security Gateway Clusters in Load Sharing mode
- B. Dedicated Log Server
- C. Dedicated SmartEvent Server
- D. Security Gateways/Clusters in ClusterXL HA new mode

Answer: D

NEW QUESTION 399

- (Exam Topic 4)

Check Point ClusterXL Active/Active deployment is used when:

- A. Only when there is Multicast solution set up.
- B. There is Load Sharing solution set up.
- C. Only when there is Unicast solution set up.
- D. There is High Availability solution set up.

Answer: D

NEW QUESTION 400

- (Exam Topic 4)

If a "ping"-packet is dropped by FW1 Policy –on how many inspection Points do you see this packet in "fw monitor"?

- A. "i", "I" and "o"
- B. I don't see it in fw monitor
- C. "i" only
- D. "i" and "I"

Answer: C

NEW QUESTION 402

- (Exam Topic 4)

Fill in the blank: _____ information is included in “Full Log” tracking option, but is not included in “Log” tracking option?

- A. Destination port
- B. Data type
- C. File attributes
- D. Application

Answer: B

NEW QUESTION 404

- (Exam Topic 4)

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 409

- (Exam Topic 4)

Which command shows the current Security Gateway Firewall chain?

- A. show current chain
- B. show firewall chain
- C. fw ctl chain
- D. fw ctl firewall-chain

Answer: C

NEW QUESTION 411

- (Exam Topic 4)

Which one of the following is NOT a configurable Compliance Regulation?

- A. GLBA
- B. CJIS
- C. SOCI
- D. NCIPA

Answer: C

NEW QUESTION 416

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

156-315.81 Practice Exam Features:

- * 156-315.81 Questions and Answers Updated Frequently
- * 156-315.81 Practice Questions Verified by Expert Senior Certified Staff
- * 156-315.81 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-315.81 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-315.81 Practice Test Here](#)