

CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81



NEW QUESTION 1

- (Exam Topic 1)

NAT rules are prioritized in which order?

- * 1. Automatic Static NAT
- * 2. Automatic Hide NAT
- * 3. Manual/Pre-Automatic NAT
- * 4. Post-Automatic/Manual NAT rules

- A. 1, 2, 3, 4
- B. 1, 4, 2, 3
- C. 3, 1, 2, 4
- D. 4, 3, 1, 2

Answer: A

NEW QUESTION 2

- (Exam Topic 1)

Which is NOT an example of a Check Point API?

- A. Gateway API
- B. Management API
- C. OPSC SDK
- D. Threat Prevention API

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

Which of the SecureXL templates are enabled by default on Security Gateway?

- A. Accept
- B. Drop
- C. NAT
- D. None

Answer: D

NEW QUESTION 4

- (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 5

- (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 6

- (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 7

- (Exam Topic 1)

Check Pnt Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____.

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

Answer: D

NEW QUESTION 8

- (Exam Topic 1)

Which command is used to set the CCP protocol to Multicast?

- A. cphaprob set_ccp multicast
- B. cphaconf set_ccp multicast
- C. cphaconf set_ccp no_broadcast
- D. cphaprob set_ccp no_broadcast

Answer: B

NEW QUESTION 9

- (Exam Topic 1)

What has to be taken into consideration when configuring Management HA?

- A. The Database revisions will not be synchronized between the management servers
- B. SmartConsole must be closed prior to synchronized changes in the objects database
- C. If you wanted to use Full Connectivity Upgrade, you must change the Implied Rules to allow FW1_cpredundant to pass before the Firewall Control Connections.
- D. For Management Server synchronization, only External Virtual Switches are supported
- E. So, if you wanted to employ Virtual Routers instead, you have to reconsider your design.

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

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 10

- (Exam Topic 1)

Fill in the blank: The R81 utility fw monitor is used to troubleshoot .

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues
- D. Phase two key negotiations

Answer: C

Explanation:

Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark.

NEW QUESTION 12

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 15

- (Exam Topic 1)

The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

- A. Secure Internal Communication (SIC)
- B. Restart Daemons if they fail
- C. Transfers messages between Firewall processes
- D. Pulls application monitoring status

Answer: D

NEW QUESTION 20

- (Exam Topic 1)

Fill in the blank: The R81 feature _____ permits blocking specific IP addresses for a specified time period.

- A. Block Port Overflow
- B. Local Interface Spoofing
- C. Suspicious Activity Monitoring
- D. Adaptive Threat Prevention

Answer: C

Explanation:

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation.

NEW QUESTION 24

- (Exam Topic 1)

Fill in the blank: The command _____ provides the most complete restoration of a R81 configuration.

- A. upgrade_import
- B. cpconfig
- C. fwm dbimport -p <export file>
- D. cpinfo -recover

Answer: A

NEW QUESTION 29

- (Exam Topic 1)

Which command will allow you to see the interface status?

- A. cphaprob interface
- B. cphaprob -l interface
- C. cphaprob -a if
- D. cphaprob stat

Answer: C

NEW QUESTION 32

- (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 35

- (Exam Topic 1)

Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

- A. UDP port 265
- B. TCP port 265
- C. UDP port 256
- D. TCP port 256

Answer: D

Explanation:

Synchronization works in two modes:

Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP connection on port 256.

Delta Sync transfers changes in the kernel tables between cluster members. Delta sync is handled by the Security Gateway kernel using UDP connections on port 8116.

NEW QUESTION 40

- (Exam Topic 1)

The Firewall Administrator is required to create 100 new host objects with different IP addresses. What API command can he use in the script to achieve the requirement?

- A. add host name <New HostName> ip-address <ip address>
- B. add hostname <New HostName> ip-address <ip address>
- C. set host name <New HostName> ip-address <ip address>
- D. set hostname <New HostName> ip-address <ip address>

Answer: A

NEW QUESTION 44

- (Exam Topic 1)

There are 4 ways to use the Management API for creating host object with R81 Management API. Which one is NOT correct?

- A. Using Web Services
- B. Using Mgmt_cli tool
- C. Using CLISH
- D. Using SmartConsole GUI console
- E. Events are collected with SmartWorkflow from Trouble Ticket systems

Answer: E

NEW QUESTION 49

- (Exam Topic 1)

What happen when IPS profile is set in Detect Only Mode for troubleshooting?

- A. It will generate Geo-Protection traffic
- B. Automatically uploads debugging logs to Check Point Support Center
- C. It will not block malicious traffic
- D. Bypass licenses requirement for Geo-Protection control

Answer: C

Explanation:

It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic.

During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.

NEW QUESTION 53

- (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 57

- (Exam Topic 1)

To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?

- A. 5 Network; Host; Objects; Services; API
- B. 3 Incoming; Outgoing; Network
- C. 2 Internal; External
- D. 4 Incoming; Outgoing; Internal; Other

Answer: D

NEW QUESTION 58

- (Exam Topic 1)

The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?

- A. fwd via cpm
- B. fwm via fwd
- C. cpm via cpd
- D. fwd via cpd

Answer: A

NEW QUESTION 62

- (Exam Topic 1)

Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 67

- (Exam Topic 1)

To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, run the following command in Expert mode then reboot:

- A. fw ctl multik set_mode 1
- B. fw ctl Dynamic_Priority_Queue on
- C. fw ctl Dynamic_Priority_Queue enable
- D. fw ctl multik set_mode 9

Answer: D

NEW QUESTION 69

- (Exam Topic 1)

Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

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

Answer: D

NEW QUESTION 72

- (Exam Topic 1)

What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

- A. Anti-Bot is the only countermeasure against unknown malware
- B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers
- C. Anti-Bot is the only signature-based method of malware protection.
- D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center.

Answer: D

NEW QUESTION 73

- (Exam Topic 1)

Which command would disable a Cluster Member permanently?

- A. clusterXL_admin down
- B. cphaprob_admin down
- C. clusterXL_admin down-p
- D. set clusterXL down-p

Answer: C

NEW QUESTION 74

- (Exam Topic 1)

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 77

- (Exam Topic 1)

If you needed the Multicast MAC address of a cluster, what command would you run?

- A. cphaprob -a if
- B. cphaconf ccp multicast
- C. cphaconf debug data
- D. cphaprob igmp

Answer: D

NEW QUESTION 81

- (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 82

- (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 83

- (Exam Topic 1)

Connections to the Check Point R81 Web API use what protocol?

- A. HTTPS
- B. RPC
- C. VPN
- D. SIC

Answer: A

NEW QUESTION 88

- (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 91

- (Exam Topic 1)

Sticky Decision Function (SDF) is required to prevent which of the following? Assume you set up an Active-Active cluster.

- A. Symmetric routing
- B. Failovers
- C. Asymmetric routing
- D. Anti-Spoofing

Answer: C

NEW QUESTION 95

- (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 97

- (Exam Topic 1)

In a Client to Server scenario, which inspection point is the first point immediately following the tables and rule base check of a packet coming from outside of the network?

- A. Big I
- B. Little o
- C. Little i
- D. Big O

Answer: A

NEW QUESTION 98

- (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 103

- (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 106

- (Exam Topic 1)

Which of the following authentication methods ARE NOT used for Mobile Access?

- A. RADIUS server
- B. Username and password (internal, LDAP)
- C. SecurID
- D. TACACS+

Answer: D

NEW QUESTION 109

- (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 110

- (Exam Topic 1)

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 111

- (Exam Topic 1)

In R81 spoofing is defined as a method of:

- A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
- B. Hiding your firewall from unauthorized users.
- C. Detecting people using false or wrong authentication logins
- D. Making packets appear as if they come from an authorized IP address.

Answer: D

Explanation:

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

NEW QUESTION 113

- (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 114

- (Exam Topic 1)

What is true about VRRP implementations?

- A. VRRP membership is enabled in cpconfig
- B. VRRP can be used together with ClusterXL, but with degraded performance
- C. You cannot have a standalone deployment
- D. You cannot have different VRIDs in the same physical network

Answer: C

NEW QUESTION 115

- (Exam Topic 2)

What are the blades of Threat Prevention?

- A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
- B. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
- C. IPS, AntiVirus, AntiBot
- D. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction

Answer: D

NEW QUESTION 117

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 119

- (Exam Topic 2)

As an administrator, you may be required to add the company logo to reports. To do this, you would save the logo as a PNG file with the name 'cover-company-logo.png' and then copy that image file to which directory on the SmartEvent server?

- A. SFWDIR/smartevent/conf
- B. \$RTDIR/smartevent/conf
- C. \$RTDIR/smartview/conf
- D. \$FWDIR/smartview/conf

Answer: C

NEW QUESTION 121

- (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 126

- (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 128

- (Exam Topic 2)

An administrator would like to troubleshoot why templating is not working for some traffic. How can he determine at which rule templating is disabled?

- A. He can use the fw accel stat command on the gateway.
- B. He can use the fw accel statistics command on the gateway.
- C. He can use the fwaccel stat command on the Security Management Server.
- D. He can use the fwaccel stat command on the gateway

Answer: D

NEW QUESTION 129

- (Exam Topic 2)

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 132

- (Exam Topic 2)

You find one of your cluster gateways showing “Down” when you run the “cphaprob stat” command. You then run the “clusterXL_admin up” on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

- A. cphaprob -f register
- B. cphaprob -d -s report
- C. cpstat -f all
- D. cphaprob -a list

Answer: D

NEW QUESTION 133

- (Exam Topic 2)

You are investigating issues with to gateway cluster members are not able to establish the first initial cluster synchronization. What service is used by the FWD daemon to do a Full Synchronization?

- A. TCP port 443
- B. TCP port 257
- C. TCP port 256
- D. UDP port 8116

Answer: C

NEW QUESTION 136

- (Exam Topic 2)

What is the protocol and port used for Health Check and State Synchronization in ClusterXL?

- A. CCP and 18190
- B. CCP and 257
- C. CCP and 8116
- D. CPC and 8116

Answer: C

NEW QUESTION 140

- (Exam Topic 2)

Can multiple administrators connect to a Security Management Server at the same time?

- A. No, only one can be connected
- B. Yes, all administrators can modify a network object at the same time
- C. Yes, every administrator has their own username, and works in a session that is independent of other administrators.
- D. Yes, but only one has the right to write.

Answer: C

NEW QUESTION 141

- (Exam Topic 2)

For Management High Availability, which of the following is NOT a valid synchronization status?

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

Answer: B

NEW QUESTION 143

- (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 148

- (Exam Topic 2)

How often does Threat Emulation download packages by default?

- A. Once a week
- B. Once an hour
- C. Twice per day
- D. Once per day

Answer: D

NEW QUESTION 149

- (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 154

- (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 155

- (Exam Topic 2)

Please choose correct command to add an "emailserver1" host with IP address 10.50.23.90 using GAIa management CLI?

- A. host name myHost12 ip-address 10.50.23.90
- B. mgmt: add host name ip-address 10.50.23.90
- C. add host name emailserver1 ip-address 10.50.23.90
- D. mgmt: add host name emailserver1 ip-address 10.50.23.90

Answer: D

NEW QUESTION 160

- (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 162

- (Exam Topic 2)

Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 163

- (Exam Topic 2)

Which command shows detailed information about VPN tunnels?

- A. cat \$FWDIR/conf/vpn.conf
- B. vpn tu tlist
- C. vpn tu
- D. cpview

Answer: B

NEW QUESTION 168

- (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 172

- (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 176

- (Exam Topic 2)

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 179

- (Exam Topic 2)

What scenario indicates that SecureXL is enabled?

- A. Dynamic objects are available in the Object Explorer
- B. SecureXL can be disabled in cpconfig
- C. fwaccel commands can be used in clish
- D. Only one packet in a stream is seen in a fw monitor packet capture

Answer: C

NEW QUESTION 180

- (Exam Topic 2)

Which Remote Access Client does not provide an Office-Mode Address?

- A. SecuRemote

- B. Endpoint Security Suite
- C. Endpoint Security VPN
- D. Check Point Mobile

Answer: A

NEW QUESTION 183

- (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 187

- (Exam Topic 2)

When gathering information about a gateway using CPINFO, what information is included or excluded when using the “-x” parameter?

- A. Includes the registry
- B. Gets information about the specified Virtual System
- C. Does not resolve network addresses
- D. Output excludes connection table

Answer: B

NEW QUESTION 188

- (Exam Topic 2)

What API command below creates a new host with the name “New Host” and IP address of “192.168.0.10”?

- A. new host name “New Host” ip-address “192.168.0.10”
- B. set host name “New Host” ip-address “192.168.0.10”
- C. create host name “New Host” ip-address “192.168.0.10”
- D. add host name “New Host” ip-address “192.168.0.10”

Answer: D

NEW QUESTION 192

- (Exam Topic 2)

With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users can perform the applications. Mobile Access encrypts all traffic using:

- A. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
- B. For end users to access the native applications, they need to install the SSL Network Extender.
- C. HTTPS for web-based applications and AES or RSA algorithm for native application
- D. For end users to access the native application, they need to install the SSL Network Extender.
- E. HTTPS for web-based applications and 3DES or RC4 algorithm for native application
- F. For end users to access the native applications, no additional software is required.
- G. HTTPS for web-based applications and AES or RSA algorithm for native application
- H. For end users to access the native application, no additional software is required.

Answer: A

NEW QUESTION 196

- (Exam Topic 2)

Which directory below contains log files?

- A. /opt/CPSmartlog-R81/log
- B. /opt/CPshrd-R81/log
- C. /opt/CPsuite-R81/fw1/log
- D. /opt/CPsuite-R81/log

Answer: C

NEW QUESTION 198

- (Exam Topic 2)

Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?

- A. mgmt_cli add-host “Server_1” ip_address “10.15.123.10” --format txt
- B. mgmt_cli add host name “Server_1” ip-address “10.15.123.10” --format json
- C. mgmt_cli add object-host “Server_1” ip-address “10.15.123.10” --format json
- D. mgmt_cli add object “Server-1” ip-address “10.15.123.10” --format json

Answer: B

Explanation:

Example:

mgmt_cli add host name "New Host 1" ip-address "192.0.2.1" --format json

- "--format json" is optional. By default the output is presented in plain text.

NEW QUESTION 202

- (Exam Topic 2)

When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of:

- A. Threat Emulation
- B. HTTPS
- C. QOS
- D. VoIP

Answer: D

NEW QUESTION 203

- (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 205

- (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 210

- (Exam Topic 2)

Customer's R81 management server needs to be upgraded to R81.10. What is the best upgrade method when the management server is not connected to the Internet?

- A. Export R81 configuration, clean install R81.10 and import the configuration
- B. CPUSE offline upgrade
- C. CPUSE online upgrade
- D. SmartUpdate upgrade

Answer: C

NEW QUESTION 212

- (Exam Topic 2)

Where do you create and modify the Mobile Access policy in R81?

- A. SmartConsole
- B. SmartMonitor
- C. SmartEndpoint
- D. SmartDashboard

Answer: A

NEW QUESTION 217

- (Exam Topic 2)

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: A

NEW QUESTION 222

- (Exam Topic 2)

What is considered Hybrid Emulation Mode?

- A. Manual configuration of file types on emulation location.
- B. Load sharing of emulation between an on premise appliance and the cloud.
- C. Load sharing between OS behavior and CPU Level emulation.
- D. High availability between the local SandBlast appliance and the cloud.

Answer: B

NEW QUESTION 225

- (Exam Topic 2)

What is the difference between SSL VPN and IPSec VPN?

- A. IPSec VPN does not require installation of a resilient 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 230

- (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 231

- (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 235

- (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 238

- (Exam Topic 2)

What is the benefit of “tw monitor” over “tcpdump”?

- A. “fw monitor” reveals Layer 2 information, while “tcpdump” acts at Layer 3.
- B. “fw monitor” is also available for 64-Bit operating systems.
- C. With “fw monitor”, you can see the inspection points, which cannot be seen in “tcpdump”
- D. “fw monitor” can be used from the CLI of the Management Server to collect information from multiple gateways.

Answer: C

NEW QUESTION 242

- (Exam Topic 2)

To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:

- A. fw ctl Dyn_Dispatch on
- B. fw ctl Dyn_Dispatch enable
- C. fw ctl multik set_mode 4
- D. fw ctl multik set_mode 1

Answer: C

NEW QUESTION 244

- (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 245

- (Exam Topic 2)

SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

- A. Analyzes each log entry as it arrives at the log server according to the Event Polic
- B. When a threat pattern is identified, an event is forwarded to the SmartEvent Server.
- C. Correlates all the identified threats with the consolidation policy.
- D. Collects syslog data from third party devices and saves them to the database.
- E. Connects with the SmartEvent Client when generating threat reports.

Answer: A

NEW QUESTION 246

- (Exam Topic 2)

Which command gives us a perspective of the number of kernel tables?

- A. fw tab -t
- B. fw tab -s
- C. fw tab -n
- D. fw tab -k

Answer: B

NEW QUESTION 248

- (Exam Topic 2)

How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

- A. cphaprob set int fwha_vmac_global_param_enabled 1
- B. clusterXL set int fwha_vmac_global_param_enabled 1
- C. fw ctl set int fwha_vmac_global_param_enabled 1
- D. cphaconf set int fwha_vmac_global_param_enabled 1

Answer: C

NEW QUESTION 252

- (Exam Topic 2)

SandBlast appliances can be deployed in the following modes:

- A. using a SPAN port to receive a copy of the traffic only
- B. detect only
- C. inline/prevent or detect
- D. as a Mail Transfer Agent and as part of the traffic flow only

Answer: C

NEW QUESTION 254

- (Exam Topic 2)

After making modifications to the \$CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

- A. cvpnd_restart
- B. cvpnd_restart
- C. cvpnd restart
- D. cvpnrestart

Answer: B

NEW QUESTION 258

- (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 259

- (Exam Topic 3)

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 260

- (Exam Topic 3)

Fill in the blank: Identity Awareness AD-Query is using the Microsoft _____ API to learn users from AD.

- A. WMI
- B. Eventvwr
- C. XML
- D. Services.msc

Answer: A

NEW QUESTION 262

- (Exam Topic 3)

Which is NOT a SmartEvent component?

- A. SmartEvent Server
- B. Correlation Unit
- C. Log Consolidator
- D. Log Server

Answer: C

NEW QUESTION 266

- (Exam Topic 3)

Joey wants to upgrade from R75.40 to R81 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this. What is one of the requirements for his success?

- A. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine
- B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine
- C. Size of the \$FWDIR/log folder of the target machine must be at least 30% of the size of the \$FWDIR/log directory on the source machine
- D. Size of the /var/log folder of the target machine must be at least 25GB or more

Answer: B

NEW QUESTION 271

- (Exam Topic 3)

What statement best describes the Proxy ARP feature for Manual NAT in R81.10?

- A. Automatic proxy ARP configuration can be enabled
- B. Translate Destination on Client Side should be configured
- C. fw ctl proxy should be configured
- D. local.arp file must always be configured

Answer: D

NEW QUESTION 274

- (Exam Topic 3)

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

NEW QUESTION 275

- (Exam Topic 3)

Please choose the path to monitor the compliance status of the Check Point R81.10 based management.

- A. Gateways & Servers --> Compliance View
- B. Compliance blade not available under R81.10

- C. Logs & Monitor --> New Tab --> Open compliance View
- D. Security & Policies --> New Tab --> Compliance View

Answer: C

NEW QUESTION 280

- (Exam Topic 3)

Which file gives you a list of all security servers in use, including port number?

- A. \$FWDIR/conf/conf.conf
- B. \$FWDIR/conf/servers.conf
- C. \$FWDIR/conf/fwauthd.conf
- D. \$FWDIR/conf/serversd.conf

Answer: C

NEW QUESTION 283

- (Exam Topic 3)

What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 287

- (Exam Topic 3)

You can access the ThreatCloud Repository from:

- A. R81.10 SmartConsole and Application Wiki
- B. Threat Prevention and Threat Tools
- C. Threat Wiki and Check Point Website
- D. R81.10 SmartConsole and Threat Prevention

Answer: D

NEW QUESTION 291

- (Exam Topic 3)

What is true of the API server on R81.10?

- A. By default the API-server is activated and does not have hardware requirements.
- B. By default the API-server is not active and should be activated from the WebUI.
- C. By default the API server is active on management and stand-alone servers with 16GB of RAM (or more).
- D. By default, the API server is active on management servers with 4 GB of RAM (or more) and on stand-alone servers with 8GB of RAM (or more).

Answer: D

NEW QUESTION 293

- (Exam Topic 3)

You have a Gateway is running with 2 cores. You plan to add a second gateway to build a cluster and used a device with 4 cores.

How many cores can be used in a Cluster for Firewall-kernel on the new device?

- A. 3
- B. 2
- C. 1
- D. 4

Answer: D

NEW QUESTION 297

- (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 302

- (Exam Topic 3)

Which process handles connection from SmartConsole R81?

- A. fwm
- B. cpmd
- C. cpm
- D. cpd

Answer: C

NEW QUESTION 304

- (Exam Topic 3)

Which file contains the host address to be published, the MAC address that needs to be associated with the IP Address, and the unique IP of the interface that responds to ARP request?

- A. /opt/CPshrd-R81/conf/local.arp
- B. /var/opt/CPshrd-R81/conf/local.arp
- C. \$CPDIR/conf/local.arp
- D. \$FWDIR/conf/local.arp

Answer: D

NEW QUESTION 306

- (Exam Topic 3)

Vanessa is firewall administrator in her company. Her company is using Check Point firewall on a central and several remote locations which are managed centrally by R77.30 Security Management Server. On central location is installed R77.30 Gateway on Open server. Remote locations are using Check Point UTM-1570 series appliances with R75.30 and some of them are using a UTM-1-Edge-X or Edge-W with latest available firmware. She is in process of migrating to R81.

What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R81?

- A. Missing an installed R77.20 Add-on on Security Management Server
- B. Unsupported firmware on UTM-1 Edge-W appliance
- C. Unsupported version on UTM-1 570 series appliance
- D. Unsupported appliances on remote locations

Answer: A

NEW QUESTION 311

- (Exam Topic 3)

Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAI/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.

What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

- A. Pamela should check SecureXL status on DMZ Security gateway and if it's turned O
- B. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
- C. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OF
- D. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
- E. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
- F. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

Answer: A

NEW QUESTION 312

- (Exam Topic 3)

What key is used to save the current CPView page in a filename format cpview_"cpview process ID".cap"number of captures"?

- A. S
- B. W
- C. C
- D. Space bar

Answer: C

NEW QUESTION 316

- (Exam Topic 3)

One of major features in R81 SmartConsole is concurrent administration.

Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

- A. A lock icon shows that a rule or an object is locked and will be available.
- B. AdminA and AdminB are editing the same rule at the same time.
- C. A lock icon next to a rule informs that any Administrator is working on this particular rule.
- D. AdminA, AdminB and AdminC are editing three different rules at the same time.

Answer: C

NEW QUESTION 319

- (Exam Topic 3)

Check Point security components are divided into the following components:

- A. GUI Client, Security Gateway, WebUI Interface
- B. GUI Client, Security Management, Security Gateway
- C. Security Gateway, WebUI Interface, Consolidated Security Logs
- D. Security Management, Security Gateway, Consolidate Security Logs

Answer: B

NEW QUESTION 324

- (Exam Topic 3)

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 327

- (Exam Topic 3)

In which formats can Threat Emulation forensics reports be viewed in?

- A. TXT, XML and CSV
- B. PDF and TXT
- C. PDF, HTML, and XML
- D. PDF and HTML

Answer: C

NEW QUESTION 328

- (Exam Topic 3)

SandBlast agent extends 0 day prevention to what part of the network?

- A. Web Browsers and user devices
- B. DMZ server
- C. Cloud
- D. Email servers

Answer: A

NEW QUESTION 333

- (Exam Topic 3)

Office mode means that:

- A. SecurID client assigns a routable MAC address
- 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 address
- F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

NEW QUESTION 334

- (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 339

- (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 344

- (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 349

- (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 351

- (Exam Topic 3)
Which NAT rules are prioritized first?

- A. Post-Automatic/Manual NAT rules
- B. Manual/Pre-Automatic NAT
- C. Automatic Hide NAT
- D. Automatic Static NAT

Answer: B

NEW QUESTION 356

- (Exam Topic 3)
Fill in the blank: Browser-based Authentication sends users to a web page to acquire identities using _____.

- A. User Directory
- B. Captive Portal and Transparent Kerberos Authentication
- C. Captive Portal
- D. UserCheck

Answer: B

NEW QUESTION 357

- (Exam Topic 3)
Which of the following commands shows the status of processes?

- A. cpwd_admin -l
- B. cpwd -l
- C. cpwd admin_list
- D. cpwd_admin list

Answer: D

NEW QUESTION 358

- (Exam Topic 3)
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. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
- C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0set static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
- D. set 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 359

- (Exam Topic 3)
In the Firewall chain mode FFF refers to:

- A. Stateful Packets
- B. No Match
- C. All Packets
- D. Stateless Packets

Answer: C

NEW QUESTION 364

- (Exam Topic 3)

The SmartEvent R81 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 369

- (Exam Topic 3)

What is the order of NAT priorities?

- A. Static NAT, IP pool NAT, hide NAT
- B. IP pool NAT, static NAT, hide NAT
- C. Static NAT, automatic NAT, hide NAT
- D. Static NAT, hide NAT, IP pool NAT

Answer: A

NEW QUESTION 370

- (Exam Topic 3)

Which of the following is NOT a VPN routing option available in a star community?

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

Answer: AD

NEW QUESTION 371

- (Exam Topic 3)

What is the SandBlast Agent designed to do?

- A. Performs OS-level sandboxing for SandBlast Cloud architecture
- B. Ensure the Check Point SandBlast services is running on the end user's system
- C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with the network
- D. Clean up email sent with malicious attachments

Answer: C

NEW QUESTION 374

- (Exam Topic 3)

What is the command to show SecureXL status?

- A. fwaccel status
- B. fwaccel stats -m
- C. fwaccel -s
- D. fwaccel stat

Answer: D

Explanation:

To check overall SecureXL status: [Expert@HostName]# fwaccel stat References:

NEW QUESTION 377

- (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 382

- (Exam Topic 3)

When using CPSTAT, what is the default port used by the AMON server?

- A. 18191
- B. 18192
- C. 18194

D. 18190

Answer: B

NEW QUESTION 386

- (Exam Topic 3)

With MTA (Mail Transfer Agent) enabled the gateways manages SMTP traffic and holds external email with potentially malicious attachments. What is required in order to enable MTA (Mail Transfer Agent) functionality in the Security Gateway?

- A. Threat Cloud Intelligence
- B. Threat Prevention Software Blade Package
- C. Endpoint Total Protection
- D. Traffic on port 25

Answer: B

NEW QUESTION 390

- (Exam Topic 3)

SmartEvent provides a convenient way to run common command line executables that can assist in investigating events. Right-clicking the IP address, source or destination, in an event provides a list of default and customized commands. They appear only on cells that refer to IP addresses because the IP address of the active cell is used as the destination of the command when run. The default commands are:

- A. ping, traceroute, netstat, and route
- B. ping, nslookup, Telnet, and route
- C. ping, whois, nslookup, and Telnet
- D. ping, traceroute, netstat, and nslookup

Answer: C

NEW QUESTION 395

- (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 398

- (Exam Topic 3)

In ClusterXL Load Sharing Multicast Mode:

- A. only the primary member received packets sent to the cluster IP address
- B. only the secondary member receives packets sent to the cluster IP address
- C. packets sent to the cluster IP address are distributed equally between all members of the cluster
- D. every member of the cluster received all of the packets sent to the cluster IP address

Answer: D

NEW QUESTION 399

- (Exam Topic 3)

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 403

- (Exam Topic 3)

Which command would you use to set the network interfaces' affinity in Manual mode?

- A. sim affinity -m
- B. sim affinity -l
- C. sim affinity -a
- D. sim affinity -s

Answer: D

NEW QUESTION 406

- (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 408

- (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 409

- (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 412

- (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 413

- (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 417

- (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 420


- (Exam Topic 3)


What does it mean if Deyra sees the gateway status? (Choose the BEST answer.)


 General


▼








 ▼

 ▼

 ▼



Status	Name	IP	Version	Active Blade
	 A-GW	10.1.1.1	R80	
	 SMS	10.1.1.101	R80	  

- A. SmartCenter Server cannot reach this Security Gateway.
- B. There is a blade reporting a problem.
- C. VPN software blade is reporting a malfunction.
- D. Security Gateway's MGNT NIC card is disconnected.

Answer: B

NEW QUESTION 423

- (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 426

- (Exam Topic 4)

Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently capable of issuing and managing certificate. Alice uses the Check Point command "cpconfig" to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances "Primary & Secondary" Which configuration option does she need to look for:

- A. Certificate's Fingerprint
- B. Random Pool
- C. CA Authority
- D. Certificate Authority

Answer: D

NEW QUESTION 429

- (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 434

- (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 438

- (Exam Topic 4)

What is the default size of NAT table fw_x_alloc?

- A. 20000
- B. 35000
- C. 25000
- D. 10000

Answer: C

NEW QUESTION 443

- (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 444

- (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 445

- (Exam Topic 4)

Which command lists firewall chain?

- A. fwctl chain
- B. fw list chain
- C. fw chain module
- D. fw tab -t chainmod

Answer: A

Explanation:

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

NEW QUESTION 449

- (Exam Topic 4)

Which Check Point daemon invokes and monitors critical processes and attempts to restart them if they fail?

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

Answer: C

NEW QUESTION 453

- (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?

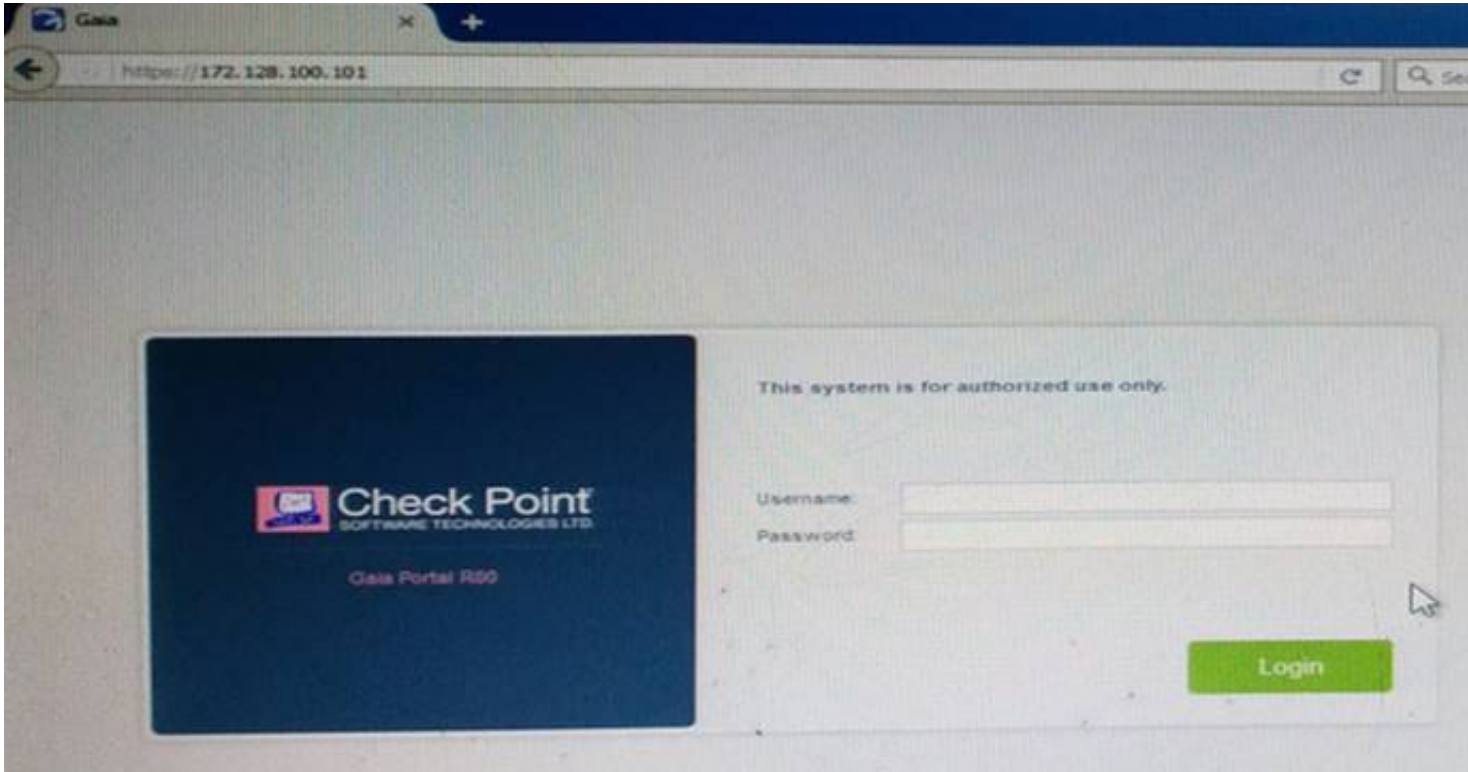
- A. run fw unloadlocal" on the relevant gateway and check the ping again
- B. run "cpstop" on the relevant gateway and check the ping again
- C. run "fw log" on the relevant gateway
- D. run "fw ctl zdebug drop" on the relevant gateway

Answer: D

NEW QUESTION 458

- (Exam Topic 4)

Kofi, the administrator of the ALPHA Corp network wishes to change the default Gaia WebUI Portal port number currently set on the default HTTPS port. Which CLISH commands are required to be able to change this TCP port?



- A. set web ssl-port <new port number>
- B. set Gaia-portal port <new port number>
- C. set Gaia-portal https-port <new port number>
- D. set web https-port <new port number>

Answer: A

NEW QUESTION 462

- (Exam Topic 4)

Which components allow you to reset a VPN tunnel?

- A. vpn tu command or SmartView monitor
- B. delete vpn ike sa or vpn she11 command
- C. vpn tunnelutil or delete vpn ike sa command
- D. SmartView monitor only

Answer: D

NEW QUESTION 467

- (Exam Topic 4)

What is the SOLR database for?

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

Answer: A

NEW QUESTION 469

- (Exam Topic 4)

When using the Mail Transfer Agent, where are the debug logs stored?

- A. \$FWDIR/bin/emaild.mt
- B. elg
- C. \$FWDIR/log/mtad elg
- D. /var/log/mail.mta elg
- E. \$CPDIR/log/emaild elg

Answer: C

NEW QUESTION 472

- (Exam Topic 4)

Which of the following Check Point commands is true to enable Multi-Version Cluster (MVC)?

- A. Check Point Security Management HA (Secondary): set cluster member mvc on
- B. Check Point Security Gateway Only: set cluster member mvc on
- C. Check Point Security Management HA (Primary): set cluster member mvc on
- D. Check Point Security Gateway Cluster Member: set cluster member mvc on

Answer: D

NEW QUESTION 473

- (Exam Topic 4)

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

- A. Access Control Policy
- B. Through the Mobile Console
- C. Shared Gateways Policy
- D. From the Dedicated Mobility Tab

Answer: B

NEW QUESTION 476

- (Exam Topic 4)

What are the modes of SandBlast Threat Emulation deployment?

- A. Cloud, Smart-1 and Hybrid
- B. Clou
- C. OpenServer and Vmware
- D. Cloud, Appliance and Private
- E. Cloud, Appliance and Hybrid

Answer: D

NEW QUESTION 477

- (Exam Topic 4)

What are the services used for Cluster Synchronization?

- A. 256H-CP for Full Sync and 8116/UDP for Delta Sync
- B. 8116/UDP for Full Sync and Delta Sync
- C. TCP/256 for Full Sync and Delta Sync
- D. No service needed when using Broadcast Mode

Answer: C

NEW QUESTION 482

- (Exam Topic 4)

Sieve is a Cyber Security Engineer working for Global Bank with a large scale deployment of Check Point Enterprise Appliances Steve's manager. Diana asks him to provide firewall connection table details from one of the firewalls for which he is responsible. Which of these commands may impact performance briefly and should not be used during heavy traffic times of day?

- A. fw tab -t connections -s
- B. fw tab -t connections
- C. fw tab -t connections -c
- D. fw tab -t connections -f

Answer: B

NEW QUESTION 487

- (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 492

- (Exam Topic 4)

You plan to automate creating new objects using new R81 Management API. You decide to use GAIA CLI for this task.

What is the first step to run management API commands on GAIA's shell?

- A. mgmt_admin@teabag > id.txt
- B. mgmt_login
- C. login user admin password teabag
- D. mgmt_cli login user "admin" password "teabag" > id.txt

Answer: B

NEW QUESTION 496

- (Exam Topic 4)

Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

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

Answer: B

NEW QUESTION 501

- (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 504

- (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 509

- (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 511

- (Exam Topic 4)

Alice & Bob are concurrently logged In via SSH on the same Check Point Security Gateway as user "admin" however Bob was first logged in and acquired the lock Alice Is not aware that Bob is also toggged in to the same Security Management Server as she is but she needs to perform very urgent configuration changes - which of the following GAIAClish command is true for overriding Bobs configuration database lock:

- A. lock database override
- B. unlock override database
- C. unlock database override
- D. database unlock override

Answer: A

NEW QUESTION 516

- (Exam Topic 4)

Matt wants to upgrade his old Security Management server to R81.x using the Advanced Upgrade with Database Migration. What is one of the requirements for a successful upgrade?

- A. Size of the /var/log folder of the source machine must be at least 25% of the size of the /var/log directory on the target machine
- B. Size of the /var/log folder of the target machine must be at least 25% of the size of the /var/log directory on the source machine
- C. Size of the \$FWDIR/log folder of the target machine must be at least 30% of the size of the \$FWDIR/log directory on the source machine
- D. Size of the /var/log folder of the target machine must be at least 25GB or more

Answer: B

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/90083

NEW QUESTION 518

- (Exam Topic 4)

Bob needs to know if Alice was configuring the new virtual cluster interface correctly. Which of the following Check Point commands is true?

- A. cphaprob-aif
- B. cp hap rob state
- C. cphaprob list
- D. probcpha -a if

Answer: A

NEW QUESTION 522

- (Exam Topic 4)

Check Point Support in many cases asks you for a configuration summary of your Check Point system. This is also called:

- A. cpexport
- B. sysinfo
- C. cpsizeme
- D. cpinfo

Answer: D

NEW QUESTION 523

- (Exam Topic 4)

What is required for a site-to-site VPN tunnel that does not use certificates?

- A. Pre-Shared Secret
- B. RSA Token
- C. Unique Passwords
- D. SecureID

Answer: A

NEW QUESTION 528

- (Exam Topic 4)

What is required for a certificate-based VPN tunnel between two gateways with separate management systems?

- A. Mutually Trusted Certificate Authorities
- B. Shared User Certificates
- C. Shared Secret Passwords
- D. Unique Passwords

Answer: A

NEW QUESTION 531

- (Exam Topic 4)

What traffic does the Anti-bot feature block?

- A. Command and Control traffic from hosts that have been identified as infected
- B. Command and Control traffic to servers with reputation for hosting malware
- C. Network traffic that is directed to unknown or malicious servers
- D. Network traffic to hosts that have been identified as infected

Answer: A

NEW QUESTION 533

- (Exam Topic 4)

GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

- A. Check Point Update Service Engine
- B. Check Point Software Update Agent
- C. Check Point Remote Installation Daemon (CPRID)
- D. Check Point Software Update Daemon

Answer: A

NEW QUESTION 536

- (Exam Topic 4)

Within the Check Point Firewall Kernel resides Chain Modules, which are individually responsible for the inspection of a specific blade or feature that has been enabled in the configuration of the gateway. For Wire mode configuration, chain modules marked with _____ will not apply.

- A. fffffff
- B. 00000001
- C. 00000002
- D. 00000003

Answer: B

NEW QUESTION 538

- (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 542

- (Exam Topic 4)

Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when _____.

- A. The license is attached to the wrong Security Gateway.
- 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 545

- (Exam Topic 4)

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 550

- (Exam Topic 4)

You need to change the MAC-address on eth2 interface of the gateway. What command and what mode will you use to achieve this goal?

- A. set interface eth2 mac-addr 11:11:11:11:11:11; CLISH
- B. ifconfig eth1 hw 11:11:11:11:11:11; expert
- C. set interface eth2 hw-addr 11:11:11:11:11:11; CLISH
- D. ethtool -i eth2 mac 11:11:11:11:11:11; expert

Answer: A

NEW QUESTION 554

- (Exam Topic 4)

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 555

- (Exam Topic 4)

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

Answer: C

NEW QUESTION 559

- (Exam Topic 4)

Alice works for a big security outsourcing provider company and as she receives a lot of change requests per day she wants to use for scripting daily (asks the API services from Check Point for the Management API. Firstly she needs to be aware if the API services are running for the management. Which of the following Check Point Command is true:

- A. api mgmt status
- B. api status
- C. status api
- D. status mgmt apt

Answer: B

NEW QUESTION 560

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 561

- (Exam Topic 4)

Which Correction mechanisms are available with ClusterXL under R81.10?

- A. Correction Mechanisms are only available of Maestro Hyperscale Orchestrators
- B. Pre-Correction and SDF (Sticky Decision Function)
- C. SDF (Sticky Decision Function) and Flush and ACK
- D. Dispatcher (Early Correction) and Firewall (Late Correction)

Answer: C

NEW QUESTION 563

- (Exam Topic 4)

Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is _____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

- A. Accept; redirect
- B. Accept; drop
- C. Redirect; drop
- D. Drop; accept

Answer: D

NEW QUESTION 566

- (Exam Topic 4)

SecureXL is able to accelerate the Connection Rate using templates. Which attributes are used in the template to identify the connection?

- A. Source address . Destination address
- B. Source Port, Destination port
- C. Source address . Destination address
- D. Destination port
- E. Source address . Destination address
- F. Destination port
- G. Protocol
- H. Source address . Destination address
- I. Source Port, Destination port
- J. Protocol

Answer: D

NEW QUESTION 568

- (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 569

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

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminGuide/R81

https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_PerformanceTuning_AdminGuide/ cpconfig -> Enter the number of the Check Point CoreXL option. (Enter 1 to select Change the number of firewall instances. OR Enter 2 for the option Change the number of IPv6 firewall instances.) -> Enter the total number of IPv4 (IPv6) CoreXL Firewall instances you wish the Security Gateway to run. Follow the instructions on the screen. -> Exit from the cpconfig menu.

- Reboot the Security Gateway.

NEW QUESTION 573

- (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 577

- (Exam Topic 4)

Which command is used to obtain the configuration lock in Gaia?

- A. Lock database override
- B. Unlock database override
- C. Unlock database lock
- D. Lock database user

Answer: A

Explanation:

Obtaining a Configuration Lock

NEW QUESTION 579

- (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 582

- (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 587

- (Exam Topic 4)

Which component is NOT required to communicate with the Web Services API?

- A. API key
- B. session ID token
- C. content-type
- D. Request payload

Answer: A

NEW QUESTION 589

- (Exam Topic 4)

What is the default shell for the command line interface?

- A. Expert
- B. Clish
- C. Admin
- D. Normal

Answer: B

Explanation:

The default shell of the CLI is called clish References:

NEW QUESTION 590

- (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 593

- (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 597

- (Exam Topic 4)

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

Answer: B

NEW QUESTION 601

- (Exam Topic 4)

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

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

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 604

- (Exam Topic 4)

What is false regarding a Management HA environment?

- A. Only one Management Server should be active, while any others be in standby mode
- B. It is not necessary to establish SIC between the primary and secondary management server, since the latter gets the exact same copy of the management database from the prior.
- C. SmartConsole can connect to any management server in Readonly mode.
- D. Synchronization will occur automatically with each Publish event if the Standby servers are available.

Answer: B

NEW QUESTION 608

- (Exam Topic 4)

When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?

- A. Network, and defining your Class A space
- B. Topology, and you are defining the Internal network
- C. Internal addresses you are defining the gateways
- D. Internal network(s) you are defining your networks

Answer: D

NEW QUESTION 611

- (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 612

- (Exam Topic 4)

When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

- A. Toni? AND 10.0.4.210 NOT 10.0.4.76
- B. To** AND 10.0.4.210 NOT 10.0.4.76
- C. Ton* AND 10.0.4.210 NOT 10.0.4.75
- D. "Toni" AND 10.0.4.210 NOT 10.0.4.76

Answer: D

NEW QUESTION 613

- (Exam Topic 4)

The Check Point history feature in R81 provides the following:

- A. View install changes and install specific version
- B. View install changes
- C. Policy Installation Date, view install changes and install specific version
- D. Policy Installation Date only

Answer: D

NEW QUESTION 618

- (Exam Topic 4)

How is communication between different Check Point components secured in R81? 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 622

- (Exam Topic 4)

Which command shows only the table names of all kernel tables?

- A. fwtab-t
- B. fw tab -s
- C. fw tab -n
- D. fw tab -k

Answer: A

NEW QUESTION 627

- (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 629

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 632

- (Exam Topic 4)

True or False: In R81, more than one administrator can login to the Security Management Server with write permission at the same time.

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

Answer: B

NEW QUESTION 634

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 635

- (Exam Topic 4)

In Advanced Permanent Tunnel Configuration, to set the amount of time the tunnel test runs without a response before the peer host is declared 'down', you would set the ?

- A. life sign polling interval
- B. life sign timeout
- C. life_sign_polling_interval
- D. life_sign_timeout

Answer: D

Explanation:

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_VPN_AdminGuide/14018

NEW QUESTION 638

- (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 639

- (Exam Topic 4)

What is Dynamic Balancing?

- A. It is a ClusterXL feature that switches an HA cluster into an LS cluster if required to maximize throughput
- B. It is a feature that uses a daemon to balance the required number of firewall instances and SNDs based on the current load
- C. It is a new feature that is capable of dynamically reserve the amount of Hash kernel memory to reflect the resource usage necessary for maximizing the session rate.
- D. It is a CoreXL feature that assigns the SND to network interfaces to balance the RX Cache of the interfaces

Answer: B

NEW QUESTION 640

- (Exam Topic 4)

To find records in the logs that shows log records from the Application & URL Filtering Software Blade where traffic was dropped, what would be the query syntax?

- A. blada: application control AND action:drop
- B. blade."application control AND action;drop
- C. (blade: application control AND action;drop)
- D. blade;"application control AND action:drop

Answer: D

NEW QUESTION 645

- (Exam Topic 4)

Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 646

- (Exam Topic 4)

According to the policy installation flow the transfer state (CPTA) is responsible for the code generated by the FWM. On the Security Gateway side a process receives them and first stores them into a temporary directory. Which process is true for receiving these Tiles;

- A. FWD
- B. CPD
- C. FWM
- D. RAD

Answer: A

NEW QUESTION 648

- (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 649

- (Exam Topic 4)

Which is the correct order of a log flow processed by SmartEvent components?

- A. Firewall > Correlation Unit > Log Server > SmartEvent Server Database > SmartEvent Client
- B. Firewall > SmartEvent Server Database > Correlation Unit > Log Server > SmartEvent Client
- C. Firewall > Log Server > SmartEvent Server Database > Correlation Unit > SmartEvent Client
- D. Firewall > Log Server > Correlation Unit > SmartEvent Server Database > SmartEvent Client

Answer: D

NEW QUESTION 653

- (Exam Topic 4)

Which software blade does NOT accompany the Threat Prevention policy?

- A. Anti-virus
- B. IPS
- C. Threat Emulation
- D. Application Control and URL Filtering

Answer: D

NEW QUESTION 655

- (Exam Topic 4)

Main Mode in IKEv1 uses how many packages for negotiation?

- A. 4
- B. depends on the make of the peer gateway
- C. 3
- D. 6

Answer: C

NEW QUESTION 656

- (Exam Topic 4)

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

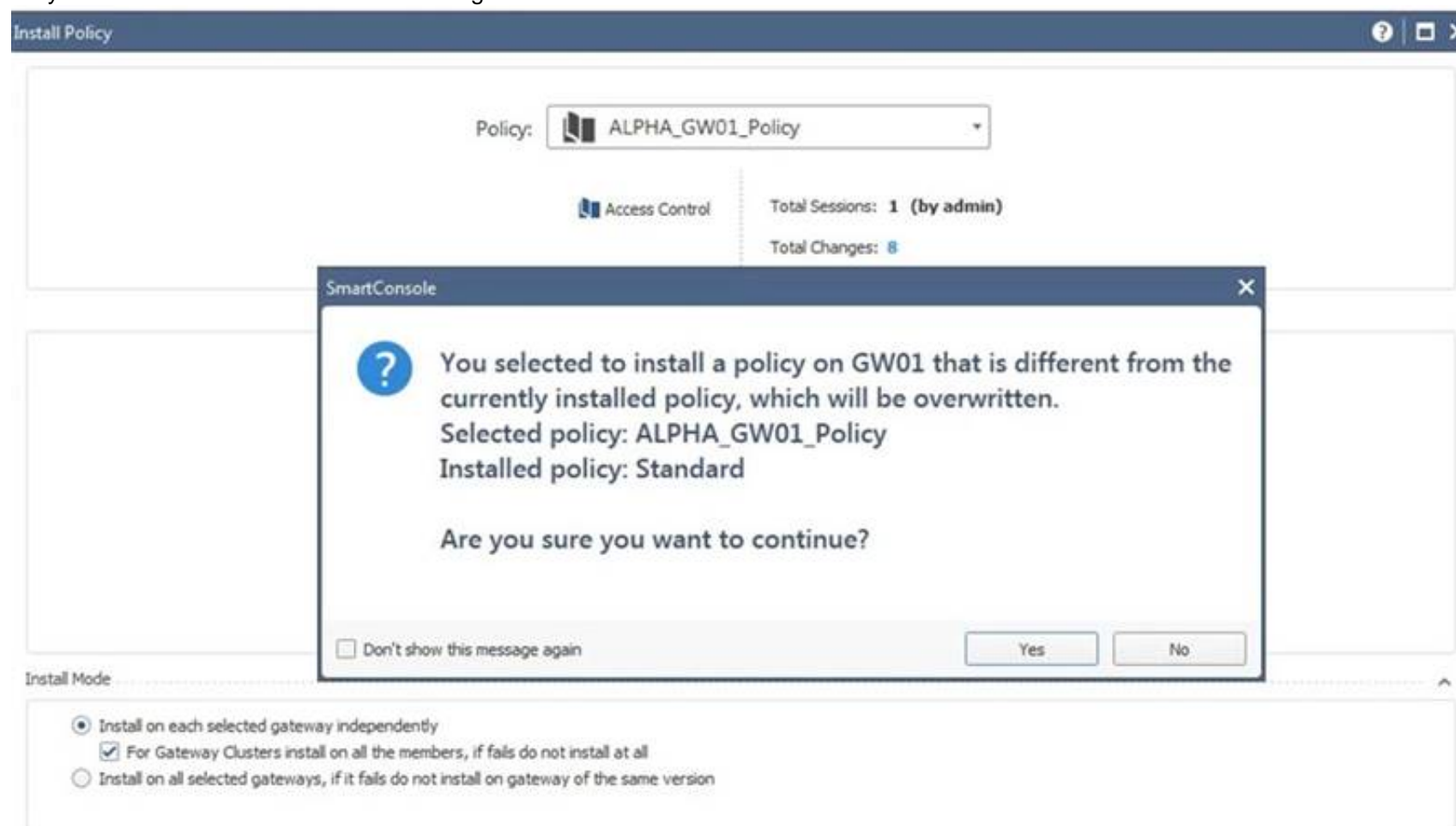
- A. Clean Install
- B. Export Package
- C. Upgrade
- D. Database Conversion to R81.10 only

Answer: B

NEW QUESTION 657

- (Exam Topic 4)

Why would an administrator see the message below?



- A. A new Policy Package created on both the Management and Gateway will be deleted and must be backed up first before proceeding.
- B. A new Policy Package created on the Management is going to be installed to the existing Gateway.
- C. A new Policy Package created on the Gateway is going to be installed on the existing Management.
- D. A new Policy Package created on the Gateway and transferred to the Management will be overwritten by the Policy Package currently on the Gateway but can be restored from a periodic backup on the Gateway.

Answer: B

NEW QUESTION 662

- (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 665

- (Exam Topic 4)

While using the Gaia CLI, what is the correct command to publish changes to the management server?

- A. json publish
- B. mgmt publish
- C. mgmt_cli commit
- D. commit

Answer: B

NEW QUESTION 670

- (Exam Topic 4)

An established connection is going to www.google.com. The Application Control Blade is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?

- A. Slow Path
- B. Fast Path
- C. Medium Path
- D. Accelerated Path

Answer: D

NEW QUESTION 671

- (Exam Topic 4)

What is the command to check the status of Check Point processes?

- A. top
- B. cptop
- C. cphaprob list
- D. cpwd_admin list

Answer: D

NEW QUESTION 676

- (Exam Topic 4)

When performing a minimal effort upgrade, what will happen to the network traffic?

- A. All connections that were Initiated before the upgrade will be dropped, causing network downtime.
- B. All connections that were initiated before the upgrade will be handled by the active gateway
- C. All connections that were initiated before the upgrade will be handled normally
- D. All connections that were initiated before the upgrade will be handled by the standby gateway

Answer: B

NEW QUESTION 677

- (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 681

- (Exam Topic 4)

What is the recommended way to have a redundant Sync connection between the cluster nodes?

- A. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per nod
- B. Connect both Sync interfaces without using a switch.
- C. Use a group of bonded interface
- D. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define a Virtual IP for the Sync interface.
- E. In the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management and define two Sync interfaces per nod
- F. Use two different Switches to connect both Sync interfaces.
- G. Use a group of bonded interfaces connected to different switche
- H. Define a dedicated sync interface, only one interface per node using the SmartConsole / Gateways & Servers -> select Cluster Properties / Network Management.

Answer: C

NEW QUESTION 686

- (Exam Topic 4)

In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom Which of the following statements is correct?

- A. If the Action of the matching rule is Accept the gateway will drop the packet
- B. If the Action of the matching rule is Drop, the gateway continues to check rules in the next Policy Layer down
- C. If the Action of the matching rule is Drop the gateway stops matching against later rules in the Policy Rule Base and drops the packet
- D. If the rule does not matched in the Network policy it will continue to other enabled polices

Answer: C

Explanation:

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

NEW QUESTION 689

- (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 691

- (Exam Topic 4)

What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?

- A. test_connectivity_ad -d <domain>

- B. test_ldap_connectivity -d <domain>
- C. test_ad_connectivity -d <domain>
- D. ad_connectivity_test -d <domain>

Answer: C

Explanation:

<https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/>

[CP_R81.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/CP_R81.30_CLI_ReferenceGuide/200877](https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/CP_R81.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/CP_R81.30_CLI_ReferenceGuide/200877)

NEW QUESTION 692

- (Exam Topic 4)

What does Backward Compatibility mean upgrading the Management Server and how can you check it?

- A. The Management Server is able to manage older Gateway
- B. The lowest supported version is documented in the Installation and Upgrade Guide
- C. The Management Server is able to manage older Gateways The lowest supported version is documented in the Release Notes
- D. You will be able to connect to older Management Server with the SmartConsol
- E. The lowest supported version is documented in the Installation and Upgrade Guide
- F. You will be able to connect to older Management Server with the SmartConsole The lowest supported version is documented in the Release Notes

Answer: A

NEW QUESTION 694

- (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 696

- (Exam Topic 4)

You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

- A. fw unloadlocal
- B. fw unloadpolicy
- C. fwm unload local
- D. fwm unload policy

Answer: A

NEW QUESTION 700

- (Exam Topic 4)

At what point is the Internal Certificate Authority (ICA) created?

- A. Upon creation of a certificate.
- B. During the primary Security Management Server installation process.
- C. When an administrator decides to create one.
- D. When an administrator initially logs into SmartConsole.

Answer: B

NEW QUESTION 701

- (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 703

- (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 707

- (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 708

- (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 711

- (Exam Topic 4)

How many interfaces can you configure to use the Multi-Queue feature?

- A. 10 interfaces
- B. 3 interfaces
- C. 4 interfaces
- D. 5 interfaces

Answer: D

NEW QUESTION 713

- (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 714

- (Exam Topic 4)

What are not possible commands to acquire the lock in order to make changes in Clish or Web GUI?

- A. set config-lock on override
- B. Click the Lock icon in the WebUI
- C. "set rbac rw = 1"
- D. lock database override

Answer: C

NEW QUESTION 719

- (Exam Topic 4)

The "MAC magic" value must be modified under the following condition:

- A. There is more than one cluster connected to the same VLAN
- B. A firewall cluster is configured to use Multicast for CCP traffic
- C. There are more than two members in a firewall cluster
- D. A firewall cluster is configured to use Broadcast for CCP traffic

Answer: D

NEW QUESTION 722

- (Exam Topic 4)

Fill in the blank: The IPS policy for pre-R81 gateways is installed during the _____ .

- A. Firewall policy install
- B. Threat Prevention policy install
- C. Anti-bot policy install
- D. Access Control policy install

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R81/CP_R81BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 723

- (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 724

- (Exam Topic 4)

Fill in the blanks: Gaia can be configured using the _____ or _____.

- A. GaiaUI; command line interface
- B. WebUI; Gaia Interface
- C. Command line interface; WebUI
- D. Gaia Interface; GaiaUI

Answer: C

NEW QUESTION 726

- (Exam Topic 4)

By default, which port does the WebUI listen on?

- A. 80
- B. 4434
- C. 443
- D. 8080

Answer: C

NEW QUESTION 727

- (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 730

- (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 731

- (Exam Topic 4)

What are the two types of tests when using the Compliance blade?

- A. Policy-based tests and Global properties
- B. Global tests and Object-based tests
- C. Access Control policy analysis and Threat Prevention policy analysis
- D. Tests conducted based on the IoC XMf file and analysis of SOLR documents

Answer: D

NEW QUESTION 734

.....

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](#)