

Exam Questions 156-315.81

Check Point Certified Security Expert R81

<https://www.2passeasy.com/dumps/156-315.81/>



NEW QUESTION 1

- (Exam Topic 1)

What are the different command sources that allow you to communicate with the API server?

- A. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services
- B. SmartConsole GUI Console, mgmt_cli Tool, Gaia CLI, Web Services
- C. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services
- D. API_cli Tool, Gaia CLI, Web Services

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

Which statement is true regarding redundancy?

- A. System Administrators know when their cluster has failed over and can also see why it failed over by using the cphaprob -f if command.
- B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
- C. Machines in a ClusterXL High Availability configuration must be synchronized.
- D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

Answer: D

NEW QUESTION 3

- (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 4

- (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 5

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 6

- (Exam Topic 1)

You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines a(n) _____ or _____ action for the file types.

- A. Inspect/Bypass
- B. Inspect/Prevent
- C. Prevent/Bypass
- D. Detect/Bypass

Answer: A

NEW QUESTION 7

- (Exam Topic 1)

Which command collects diagnostic data for analyzing customer setup remotely?

- A. cpinfo

- B. migrate export
- C. sysinfo
- D. cpview

Answer: A

Explanation:

CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

NEW QUESTION 8

- (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 9

- (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 10

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 10

- (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 12

- (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 16

- (Exam Topic 1)

What is the mechanism behind Threat Extraction?

- A. This a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender.
- B. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient.
- C. This is a new mechanism to identify the IP address of the sender of malicious codes and put it into the SAM database (Suspicious Activity Monitoring).
- D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast.

Answer: D

NEW QUESTION 17

- (Exam Topic 1)

Fill in the blank: The tool _____ generates a R81 Security Gateway configuration report.

- A. infoCP
- B. infoview
- C. cpinfo
- D. fw cpinfo

Answer: C

NEW QUESTION 21

- (Exam Topic 1)

What Factor preclude Secure XL Templating?

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

Answer: A

NEW QUESTION 26

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 30

- (Exam Topic 1)

Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

- A. Check Point Remote User
- B. Check Point Capsule Workspace
- C. Check Point Mobile Web Portal
- D. Check Point Capsule Remote

Answer: C

NEW QUESTION 35

- (Exam Topic 1)

During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

- A. Host having a Critical event found by Threat Emulation
- B. Host having a Critical event found by IPS
- C. Host having a Critical event found by Antivirus
- D. Host having a Critical event found by Anti-Bot

Answer: D

NEW QUESTION 36

- (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 37

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 41

- (Exam Topic 1)

SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their data. Which component is NOT part of the SandBlast Mobile solution?

- A. Management Dashboard
- B. Gateway
- C. Personal User Storage
- D. Behavior Risk Engine

Answer: C

NEW QUESTION 43

- (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 47

- (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 50

- (Exam Topic 1)

What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

- A. Stateful Mode
- B. VPN Routing Mode
- C. Wire Mode
- D. Stateless Mode

Answer: C

Explanation:

Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

NEW QUESTION 51

- (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 56

- (Exam Topic 1)

Session unique identifiers are passed to the web api using which http header option?

- A. X-chkp-sid
- B. Accept-Charset
- C. Proxy-Authorization
- D. Application

Answer: C

NEW QUESTION 58

- (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 61

- (Exam Topic 1)

Which command lists all tables in Gaia?

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

Answer: C

NEW QUESTION 64

- (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 66

- (Exam Topic 1)

Where you can see and search records of action done by R81 SmartConsole administrators?

- A. In SmartView Tracker, open active log
- B. In the Logs & Monitor view, select "Open Audit Log View"
- C. In SmartAuditLog View
- D. In Smartlog, all logs

Answer: B

NEW QUESTION 68

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 73

- (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 75

- (Exam Topic 1)

To fully enable Dynamic Dispatcher on a Security Gateway:

- A. run fw ctl multik set_mode 9 in Expert mode and then Reboot.
- B. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXL menu.
- C. Edit/proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot.
- D. run fw multik set_mode 1 in Expert mode and then reboot.

Answer: A

NEW QUESTION 79

- (Exam Topic 1)

CoreXL is supported when one of the following features is enabled:

- A. Route-based VPN
- B. IPS
- C. IPv6
- D. Overlapping NAT

Answer: B

Explanation:

CoreXL does not support Check Point Suite with these features: References:

NEW QUESTION 81

- (Exam Topic 1)

What are the attributes that SecureXL will check after the connection is allowed by Security Policy?

- A. Source address, Destination address, Source port, Destination port, Protocol
- B. Source MAC address, Destination MAC address, Source port, Destination port, Protocol
- C. Source address, Destination address, Source port, Destination port
- D. Source address, Destination address, Destination port, Protocol

Answer: A

NEW QUESTION 82

- (Exam Topic 2)

Which of these is an implicit MEP option?

- A. Primary-backup
- B. Source address based
- C. Round robin
- D. Load Sharing

Answer: A

NEW QUESTION 83

- (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 86

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 91

- (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 94

- (Exam Topic 2)

Which GUI client is supported in R81?

- A. SmartProvisioning
- B. SmartView Tracker
- C. SmartView Monitor
- D. SmartLog

Answer: C

NEW QUESTION 96

- (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 100

- (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 103

- (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 104

- (Exam Topic 2)

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

- A. Install appliance TE250X on SpanPort on LAN switch in MTA mode.
- B. Install appliance TE250X in standalone mode and setup MTA.
- C. You can utilize only Check Point Cloud Services for this scenario.
- D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance.

Answer: C

NEW QUESTION 106

- (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 111

- (Exam Topic 2)

Which encryption algorithm is the least secured?

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

Answer: C

NEW QUESTION 112

- (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 117

- (Exam Topic 2)

What is a best practice before starting to troubleshoot using the “fw monitor” tool?

- A. Run the command: fw monitor debug on
- B. Clear the connections table
- C. Disable CoreXL
- D. Disable SecureXL

Answer: D

NEW QUESTION 118

- (Exam Topic 2)

How do Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VP
- B. Capsule Workspace provides a Desktop with usable applications.
- C. Capsule Workspace can provide access to any application.
- D. Capsule Connect provides Business data isolation.
- E. Capsule Connect does not require an installed application at client.

Answer: A

NEW QUESTION 120

- (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 123

- (Exam Topic 2)

Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

- A. enable DLP and select.exe and .bat file type
- B. enable .exe & .bat protection in IPS Policy
- C. create FW rule for particular protocol
- D. tecli advanced attributes set prohibited_file_types exe.bat

Answer:

A

NEW QUESTION 126

- (Exam Topic 2)

When simulating a problem on ClusterXL cluster with cphaprob -d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

- A. cphaprob -d STOP unregister
- B. cphaprob STOP unregister
- C. cphaprob unregister STOP
- D. cphaprob -d unregister STOP

Answer: A

Explanation:

esting a failover in a controlled manner using following command;

```
# cphaprob -d STOP -s problem -t 0 register
```

This will register a problem state on the cluster member this was entered on; If you then run;

```
# cphaprob list
```

this will show an entry named STOP.

to remove this problematic register run following;

```
# cphaprob -d STOP unregister
```

 References:

NEW QUESTION 131

- (Exam Topic 2)

VPN Link Selection will perform the following when the primary VPN link goes down?

- A. The Firewall will drop the packets.
- B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
- C. The Firewall will send out the packet on all interfaces.
- D. The Firewall will inform the client that the tunnel is down.

Answer: B

NEW QUESTION 134

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 139

- (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 143

- (Exam Topic 2)

What is the purpose of Priority Delta in VRRP?

- A. When a box up, Effective Priority = Priority + Priority Delta
- B. When an Interface is up, Effective Priority = Priority + Priority Delta
- C. When an Interface fail, Effective Priority = Priority – Priority Delta
- D. When a box fail, Effective Priority = Priority – Priority Delta

Answer: C

Explanation:

Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP.

If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP

HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will begin to send out its own HELLO packet.

Once the master sees this packet with a priority greater than its own, then it releases the VIP. References:

NEW QUESTION 148

- (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 152

- (Exam Topic 2)

Which one of the following is true about Threat Extraction?

- A. Always delivers a file to user
- B. Works on all MS Office, Executables, and PDF files
- C. Can take up to 3 minutes to complete
- D. Delivers file only if no threats found

Answer: A

NEW QUESTION 153

- (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 158

- (Exam Topic 2)

Which one of the following is true about Capsule Connect?

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

Answer: A

NEW QUESTION 159

- (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 162

- (Exam Topic 2)

Which command is used to display status information for various components?

- A. show all systems
- B. show system messages
- C. sysmess all
- D. show sysenv all

Answer: D

NEW QUESTION 167

- (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 171

- (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 173

- (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 175

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 177

- (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 180

- (Exam Topic 2)

What is the port used for SmartConsole to connect to the Security Management Server?

- A. CPML port 18191/TCP
- B. CPM port/TCP port 19009
- C. SIC port 18191/TCP
- D. https port 4434/TCP

Answer: A

NEW QUESTION 185

- (Exam Topic 2)

To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

- A. Accept Template
- B. Deny Template
- C. Drop Template
- D. NAT Template

Answer: B

NEW QUESTION 190

- (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 194

- (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 195

- (Exam Topic 3)

When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

- A. All UDP packets
- B. All IPv6 Traffic
- C. All packets that match a rule whose source or destination is the Outside Corporate Network
- D. CIFS packets

Answer: D

NEW QUESTION 196

- (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 199

- (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 202

- (Exam Topic 3)

What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 207

- (Exam Topic 3)

Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.

What will happen to the changes already made?

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

Answer: A

NEW QUESTION 209

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 212

- (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 216

- (Exam Topic 3)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 220

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 222

- (Exam Topic 3)

What is the minimum amount of RAM needed for a Threat Prevention Appliance?

- A. 6 GB
- B. 8GB with Gaia in 64-bit mode
- C. 4 GB
- D. It depends on the number of software blades enabled

Answer: C

NEW QUESTION 226

- (Exam Topic 3)

Fill in the blanks. There are _____ types of software containers: _____.

- A. Three; security management, Security Gateway, and endpoint security
- B. Three; Security Gateway, endpoint security, and gateway management
- C. Two; security management and endpoint security
- D. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 228

- (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 233

- (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 237

- (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 241

- (Exam Topic 3)

Fill in the blank: The R81 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

- A. SmartMonitor
- B. SmartView Web Application
- C. SmartReporter
- D. SmartTracker

Answer: B

NEW QUESTION 245

- (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 247

- (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 250

- (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 253

- (Exam Topic 3)

Which blades and or features are not supported in R81?

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

Answer: A

NEW QUESTION 258

- (Exam Topic 3)

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

- A. ThreatWiki
- B. Whitelist Files
- C. AppWiki
- D. IPS Protections

Answer: B

NEW QUESTION 261

- (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 264

- (Exam Topic 3)

What is correct statement about Security Gateway and Security Management Server failover in Check Point R81.X in terms of Check Point Redundancy driven solution?

- A. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.
- B. Security Gateway failover as well as Security Management Server failover is a manual procedure.
- C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
- D. Security Gateway failover as well as Security Management Server failover is an automatic procedure.

Answer: A

NEW QUESTION 265

- (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 267

- (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 272

- (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 277

- (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 278

- (Exam Topic 3)

The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated.

What is the most likely reason that the traffic is not accelerated?

- A. There is a virus found
- B. Traffic is still allowed but not accelerated.
- C. The connection required a Security server.
- D. Acceleration is not enabled.
- E. The traffic is originating from the gateway itself.

Answer: B

NEW QUESTION 279

- (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 281

- (Exam Topic 3)

How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 283

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 285

- (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 286

- (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 289

- (Exam Topic 3)

Which is NOT an example of a Check Point API?

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

Answer: A

NEW QUESTION 293

- (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 298

- (Exam Topic 4)

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

Answer: B

NEW QUESTION 302

- (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 305

- (Exam Topic 4)

If the Active Security Management Server fails or if it becomes necessary to change the Active to Standby, the following steps must be taken to prevent data loss. Providing the Active Security Management Server is responsive, which if these steps should NOT be performed:

- A. Rename the hostname of the Standby member to match exactly the hostname of the Active member.
- B. Change the Standby Security Management Server to Active.
- C. Change the Active Security Management Server to Standby.
- D. Manually synchronize the Active and Standby Security Management Servers.

Answer: A

NEW QUESTION 307

- (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 308

- (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 312

- (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 315

- (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 316

- (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 318

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 319

- (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 320

- (Exam Topic 4)

The customer has about 150 remote access user with a Windows laptops. Not more than 50 Clients will be connected at the same time. The customer want to use multiple VPN Gateways as entry point and a personal firewall. What will be the best license for him?

- A. He will need Capsule Connect using MEP (multiple entry points).
- B. Because the customer uses only Windows clients SecuRemote will be sufficient and no additional license is needed
- C. He will need Harmony Endpoint because of the personal firewall.
- D. Mobile Access license because he needs only a 50 user license, license count is per concurrent use

Answer: D

NEW QUESTION 322

- (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 326

- (Exam Topic 4)

Kurt is planning to upgrade his Security Management Server to R81.X. What is the lowest supported version of the Security Management he can upgrade from?

- A. R76 Splat
- B. R77.X Gaia
- C. R75 Splat
- D. R75 Gaia

Answer: D

NEW QUESTION 329

- (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 334

- (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 338

- (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 340

- (Exam Topic 4)

When defining QoS global properties, which option below is not valid?

- A. Weight
- B. Authenticated timeout
- C. Schedule
- D. Rate

Answer: D

NEW QUESTION 341

- (Exam Topic 4)

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

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

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

Answer: D

NEW QUESTION 344

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 348

- (Exam Topic 4)

Hit Count is a feature to track the number of connections that each rule matches, which one is not benefit of Hit Count.

- A. Better understand the behavior of the Access Control Policy
- B. Improve Firewall performance - You can move a rule that has hot count to a higher position in the Rule Base
- C. Automatically rearrange Access Control Policy based on Hit Count Analysis
- D. Analyze a Rule Base - You can delete rules that have no matching connections

Answer: C

NEW QUESTION 350

- (Exam Topic 4)

In Threat Prevention, you can create new or clone profiles but you CANNOT change the out-of-the-box profiles of:

- A. Basic, Optimized, Strict
- B. Basic, Optimized, Severe
- C. General, Escalation, Severe
- D. General, purposed, Strict

Answer: A

NEW QUESTION 353

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 358

- (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 359

- (Exam Topic 4)

What is the purpose of the command "ps aux | grep twd"?

- A. You can check the Process ID and the processing time of the twd process.
- B. You can convert the log file into Post Script format.
- C. You can list all Process IDs for all running services.
- D. You can check whether the IPS default setting is set to Detect or Prevent mode

Answer: A

NEW QUESTION 362

- (Exam Topic 4)

What are the correct steps upgrading a HA cluster (M1 is active. M2 is passive) using Multi-Version Cluster(MVC) Upgrade?

- A. 1) Enable the MVC mechanism on both cluster members «cphaprob mvc on2) Upgrade the passive node M2 to R81.103) In SmartConsol
- B. change the version of the cluster object4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism
- C. 1) Enable the MVC mechanism on both cluster members #cphaprob mvc on2) Upgrade the passive node M2 to R81.103) In SmartConsol
- D. change the version of the cluster object4) Install the Access Control Policy5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy
- E. 1) In SmartConsol
- F. change the version of the cluster object2) Upgrade the passive node M2 to R81.103) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 Wcphaconf mvc on4) Install the Access Control Policy and make sure that the installation will not stop if installation on one cluster member fails5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy SmartConsol
- G. change the version of the cluster object
- H. 1) Upgrade the passive node M2 to R81.102) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 ttcphaconf mvc on3) In SmartConsole, change the version of the cluster object 4) Install the Access Control Policy5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.10

Answer: D

NEW QUESTION 364

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 367

- (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 370

- (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 374

- (Exam Topic 4)

You need to change the MAC-address on eth2 interface of the gateway. What is the correct way to change MAC-address in Check Point Gaia?

- A. In CLISH run: set interface eth2 mac-addr 11:11:11:11:11:11
- B. In expert-mode run ifconfig eth1 hw 11:11:11:11 11 11
- C. In CLISH run set interface eth2 hw-addr 11 11 11:11:11 11
- D. In expert-mode run: ethtool -4 eth2 mac 11 11:11:11:11:11

Answer: A

NEW QUESTION 375

- (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 380

- (Exam Topic 4)

What feature allows Remote-access VPN users to access resources across a site-to-site VPN tunnel?

- A. Specific VPN Communities
- B. Remote Access VPN Switch
- C. Mobile Access VPN Domain
- D. Network Access VPN Domain

Answer: B

NEW QUESTION 385

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 389

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 391

- (Exam Topic 4)

Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 396

- (Exam Topic 4)

Which of the following statements about SecureXL NAT Templates is true?

- A. NAT Templates are generated to achieve high session rate for NA
- B. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
- C. These are enabled by default and work only if Accept Templates are enabled.
- D. DROP Templates are generated to achieve high session rate for NA
- E. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
- F. These are disabled by default and work only if NAT Templates are disabled.
- G. NAT Templates are generated to achieve high session rate for NA
- H. These templates store the NAT attributes of connections matched by rulebase so that similar newconnections can take advantage of this information and do NAT without the expensive rulebase looku
- I. These are disabled by default and work only if Accept Templates are disabled.
- J. ACCEPT Templates are generated to achieve high session rate for NA
- K. These templates store the NAT attributes of connections matched by rulebase so that similar new connections can take advantage of this information and do NAT without the expensive rulebase looku
- L. These are disabled by default and work only if NAT Templates are disabled.

Answer: A

NEW QUESTION 399

- (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 403

- (Exam Topic 4)

Which of the following is NOT supported by CPUSE?

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

Answer: D

Explanation:

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

NEW QUESTION 408

- (Exam Topic 4)

In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

- A. Limit
- B. Resource
- C. Custom Application / Site
- D. Network Object

Answer: B

NEW QUESTION 411

- (Exam Topic 4)

Which process is used mainly for backward compatibility of gateways in R81.X? It provides communication with GUI-client, database manipulation, policy compilation and Management HA synchronization.

- A. cpm
- B. fwd
- C. cpd
- D. fwmD18912E1457D5D1DDCBD40AB3BF70D5D

Answer: D

NEW QUESTION 414

- (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 415

- (Exam Topic 4)

What are the two high availability modes?

- A. Load Sharing and Legacy
- B. Traditional and New
- C. Active and Standby
- D. New and Legacy

Answer: D

Explanation:

ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

NEW QUESTION 417

- (Exam Topic 4)

When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

- A. Syslog
- B. SNMPTrap
- C. Block Source
- D. Mail

Answer: B

NEW QUESTION 422

- (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 425

- (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 429

- (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 433

- (Exam Topic 4)

What is the minimum number of CPU cores required to enable CoreXL?

- A. 1
- B. 6
- C. 2
- D. 4

Answer: C

Explanation:

Default number of CoreXL IPv4 FW instances:

Note: The real number of CoreXL FW instances depends on the current CoreXL license. Number of CPU cores Default number of CoreXL IPv4

FW instances Default number of Secure Network Distributors (SNDs)

1 1

Note: CoreXL is disabled 0 Note: CoreXL is disabled

2 2 2

4 3 1

6 - 20 [Number of CPU cores] - 2 2

More than 20 (1) [Number of CPU cores] - 4 4

NEW QUESTION 436

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 440

- (Exam Topic 4)

What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?

- A. Idle <20%
- B. USR <20%
- C. SYS <20%
- D. Wait <20%

Answer: A

NEW QUESTION 445

- (Exam Topic 4)

When synchronizing clusters, which of the following statements is FALSE?

- A. The state of connections using resources is maintained in a Security Server, so their connections cannot be synchronized.
- B. Only cluster members running on the same OS platform can be synchronized.
- C. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
- D. Client Authentication or Session Authentication connections through a cluster member will be lost if the cluster member fails.

Answer: D

NEW QUESTION 450

- (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 453

- (Exam Topic 4)

The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and which port is used?

- A. In expert mode run #netstat -tulnp | grep httpd to see if httpd is up and to get the port number
- B. In dish run >show web daemon-enable to see if the web daemon is enabled.
- C. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in use
- D. In expert mode run #netstat -anp | grep httpd to see if the httpd is up
- E. In dish run >show web ssl-port to see if the web daemon is enabled and which port is in use
- F. In expert mode run #netstat -anp | grep httpd2 to see if the httpd2 is up
- G. In expert mode run #netstat -tulnp | grep httpd2 to see if httpd2 is up and to get the port number
- H. In dish run >show web daemon-enable to see if the web daemon is enabled.

Answer: C

NEW QUESTION 456

- (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 459

- (Exam Topic 4)

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

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

D. ping

Answer: C

NEW QUESTION 461

- (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 464

- (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 466

- (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 471

- (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 473

- (Exam Topic 4)

Is it possible to establish a VPN before the user login to the Endpoint Client?

- A. yes, you had to set neo_remember_user_password to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_remember_user_passwordattribute in the trac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway
- B. no, the user must login first.
- C. ye
- D. you had to set neo_always_connected to true in the trac.defaults of the Remote Access Client or you can use the endpoint_vpn_always_connected attribute in thetrac_client_1 .ttm file located in the SFWDIR/conf directory on the Security Gateway
- E. yes, you had to enable Machine Authentication in the Gateway object of the Smart Console

Answer: D

NEW QUESTION 475

- (Exam Topic 4)

What state is the Management HA in when both members have different policies/databases?

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

Answer:

D

Explanation:

https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/98838

NEW QUESTION 476

- (Exam Topic 4)

What is false regarding prerequisites for the Central Deployment usage?

- A. The administrator must have write permission on SmartUpdate
- B. Security Gateway must have the latest CPUSE Deployment Agent
- C. No need to establish SIC between gateways and the management server, since the CDT tool will take care about SIC automatically.
- D. The Security Gateway must have a policy installed

Answer: D

NEW QUESTION 478

- (Exam Topic 4)

What API command below creates a new host object with the name "My Host" and IP address of "192 168 0 10"?

- A. set host name "My Host" ip-address "192.168.0.10"
- B. new host name "My Host" ip-address "192 168.0.10"
- C. create host name "My Host" ip-address "192.168 0.10"
- D. mgmt.cli -m <mgmt ip> add host name "My Host" ip-address "192.168.0 10"

Answer: A

NEW QUESTION 479

- (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?

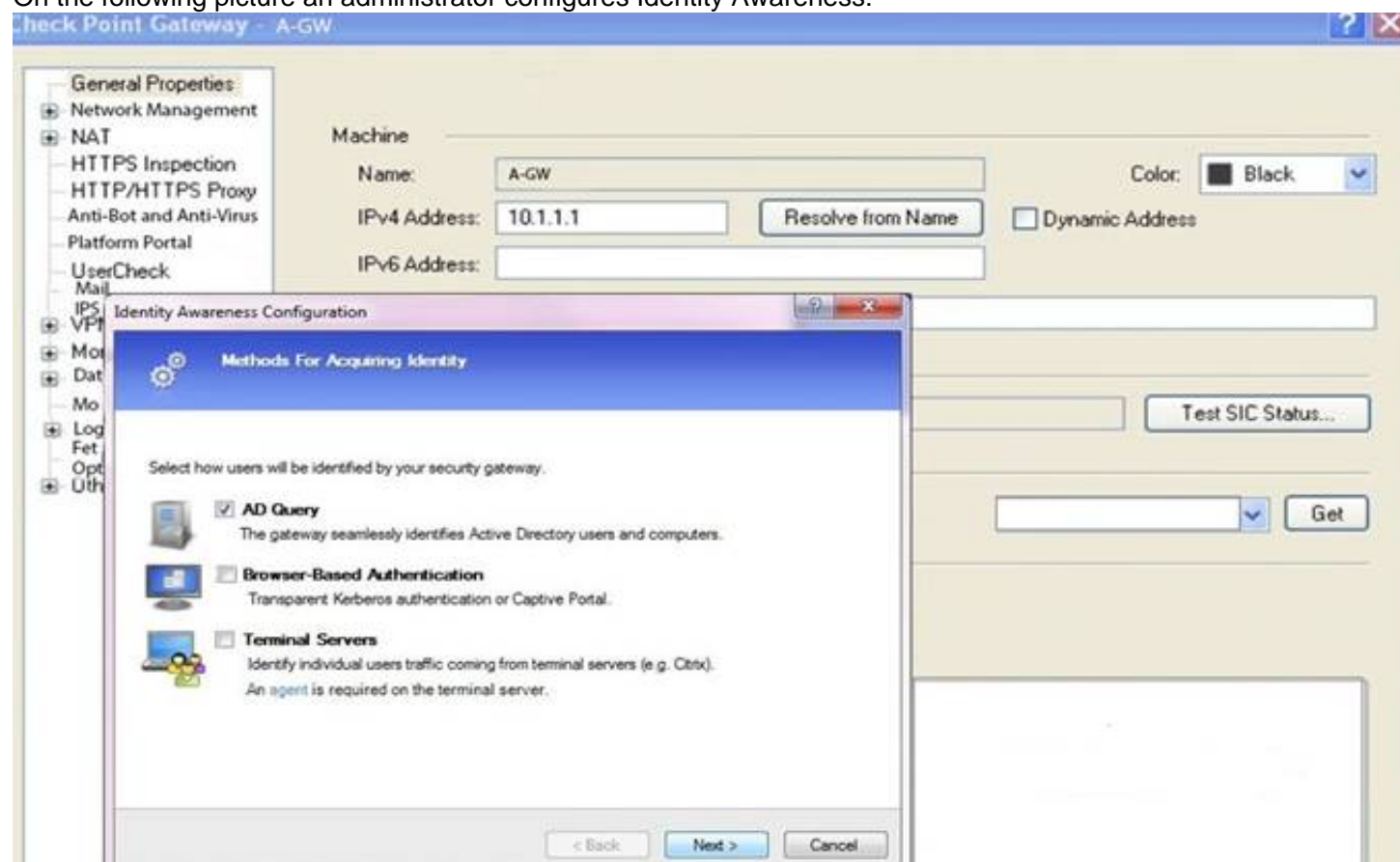
- A. Slow Path
- B. Fast Path
- C. Medium Path
- D. Accelerated Path

Answer: D

NEW QUESTION 481

- (Exam Topic 4)

On the following picture an administrator configures Identity Awareness:



After clicking "Next" the above configuration is supported by:

- A. Kerberos SSO which will be working for Active Directory integration
- B. Based on Active Directory integration which allows the Security Gateway to correlate Active Directory users and machines to IP addresses in a method that is completely transparent to the user.
- C. Obligatory usage of Captive Portal.
- D. The ports 443 or 80 what will be used by Browser-Based and configured Authentication.

Answer: B

NEW QUESTION 484

- (Exam Topic 4)

How can you see historical data with cpview?

- A. cpview -f <timestamp>
- B. cpview -e <timestamp>
- C. cpview -t <timestamp>
- D. cpview -d <timestamp>

Answer: C

NEW QUESTION 489

- (Exam Topic 4)

What is the best method to upgrade a Security Management Server to R81.x when it is not connected to the Internet?

- A. CPUSE offline upgrade only
- B. Advanced upgrade or CPUSE offline upgrade
- C. Advanced Upgrade only
- D. SmartUpdate offline upgrade

Answer: B

NEW QUESTION 494

- (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 499

- (Exam Topic 4)

Aaron is a Syber Security Engineer working for Global Law Firm with large scale deployment of Check Point Enterprise Appliances running GAiA R81.X The Network Security Developer Team is having an issue testing the API with a newly deployed R81.X Security Management Server Aaron wants to confirm API services are working properly. What should he do first?

- A. Aaron should check API Server status with "fwm api status" from Expert mode If services are stopped, he should start them with "fwm api start".
- B. Aaron should check API Server status with "cpapi status" from Expert mod
- C. If services are stopped, he should start them with "cpapi start"
- D. Aaron should check API Server status with "api status" from Expert mode If services are stopped, he should start them with "api start"
- E. Aaron should check API Server status with "cpm api status" from Expert mod
- F. If services are stopped, he should start them with "cpi api start".

Answer: C

NEW QUESTION 500

- (Exam Topic 4)

What mechanism can ensure that the Security Gateway can communicate with the Management Server with ease in situations with overwhelmed network resources?

- A. The corresponding feature is new to R81.10 and is called "Management Data Plane Separation"
- B. The corresponding feature is called "Dynamic Dispatching"
- C. There is a feature for ensuring stable connectivity to the management server and is done via Priority Queuing.
- D. The corresponding feature is called "Dynamic Split"

Answer: A

NEW QUESTION 503

- (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 508

- (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 512

- (Exam Topic 4)

What are possible Automatic Reactions in SmartEvent?

- A. Mail
- B. SNMP Trap, Block Source
- C. Block Event Activity, External Script
- D. Web Mail
- E. Block Destination, SNMP Trap
- F. SmartTask
- G. Web Mail, Block Service
- H. SNMP Trap
- I. SmartTask, Geo Protection
- J. Web Mail, Forward to SandBlast Appliance, SNMP Trap, External Script

Answer: A

NEW QUESTION 514

- (Exam Topic 4)

What is the amount of Priority Queues by default?

- A. There are 8 priority queues and this number cannot be changed.
- B. There is no distinct number of queues since it will be changed in a regular basis based on its system requirements.
- C. There are 7 priority queues by default and this number cannot be changed.
- D. There are 8 priority queues by default, and up to 8 additional queues can be manually configured

Answer: D

NEW QUESTION 519

- (Exam Topic 4)

Which Check Point software blade provides protection from zero-day and undiscovered threats?

- A. Firewall
- B. Threat Emulation
- C. Application Control
- D. Threat Extraction

Answer: B

NEW QUESTION 524

- (Exam Topic 4)

What command is used to manually failover a cluster during a zero downtime upgrade?

- A. set cluster member down
- B. cpstop
- C. clusterXL_admin down
- D. set clusterXL down

Answer: C

NEW QUESTION 526

- (Exam Topic 4)

SmartEvent uses its 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 529

- (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 531

- (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 533

- (Exam Topic 4)

Fill in the blank: Authentication rules are defined for _____ .

- A. User groups
- B. Users using UserCheck
- C. Individual users
- D. All users in the database

Answer: A

NEW QUESTION 535

- (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 538

- (Exam Topic 4)

Which is the command to identify the NIC driver before considering about the employment of the Multi-Queue feature?

- A. show interface eth0 mq
- B. ethtool A eth0
- C. ifconfig -i eth0 verbose
- D. ip show Int eth0

Answer: A

NEW QUESTION 540

- (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 XMfifile and analysis of SOLR documents

Answer: D

NEW QUESTION 545

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 156-315.81 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 156-315.81 Product From:

<https://www.2passeasy.com/dumps/156-315.81/>

Money Back Guarantee

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