

# 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 of these statements describes the Check Point ThreatCloud?

- A. Blocks or limits usage of web applications
- B. Prevents or controls access to web sites based on category
- C. Prevents Cloud vulnerability exploits
- D. A worldwide collaborative security network

**Answer:** D

#### NEW QUESTION 3

- (Exam Topic 1)

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

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

**Answer:** A

#### NEW QUESTION 4

- (Exam Topic 1)

What is true about the IPS-Blade?

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

**Answer:** A

#### NEW QUESTION 5

- (Exam Topic 1)

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

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

**Answer:** B

#### NEW QUESTION 6

- (Exam Topic 1)

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 7

- (Exam Topic 1)

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

- A. TCP 18211

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

**Answer:** D

#### NEW QUESTION 8

- (Exam Topic 1)

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 9

- (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 10

- (Exam Topic 1)

What Factor preclude Secure XL Templating?

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

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 1)

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 12

- (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 17

- (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 19

- (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 20

- (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 24

- (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 28

- (Exam Topic 1)

What is the limitation of employing Sticky Decision Function?

- A. With SDF enabled, the involved VPN Gateways only supports IKEv1
- B. Acceleration technologies, such as SecureXL and CoreXL are disabled when activating SDF
- C. With SDF enabled, only ClusterXL in legacy mode is supported
- D. With SDF enabled, you can only have three Sync interfaces at most

**Answer:** B

#### NEW QUESTION 31

- (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 32

- (Exam Topic 1)

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

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

**Answer:** C

**Explanation:**

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

**NEW QUESTION 36**

- (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 37**

- (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 39**

- (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 40**

- (Exam Topic 1)

Identify the API that is not supported by Check Point currently.

- A. R81 Management API
- B. Identity Awareness Web Services API
- C. Open REST API
- D. OPSEC SDK

**Answer: C**

**NEW QUESTION 45**

- (Exam Topic 1)

When doing a Stand-Alone Installation, you would install the Security Management Server with which other Check Point architecture component?

- A. None, Security Management Server would be installed by itself.
- B. SmartConsole
- C. SecureClient
- D. Security Gateway
- E. SmartEvent

**Answer: D**

**NEW QUESTION 47**

- (Exam Topic 1)

Which of the following statements is TRUE about R81 management plug-ins?

- A. The plug-in is a package installed on the Security Gateway.
- B. Installing a management plug-in requires a Snapshot, just like any upgrade process.
- C. A management plug-in interacts with a Security Management Server to provide new features and support for new products.
- D. Using a plug-in offers full central management only if special licensing is applied to specific features of the plug-in.

**Answer: C**

**NEW QUESTION 52**

- (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 53**

- (Exam Topic 1)

R81.10 management server can manage gateways with which versions installed?

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

**Answer:** C

**NEW QUESTION 56**

- (Exam Topic 1)

What SmartEvent component creates events?

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

**Answer:** B

**NEW QUESTION 58**

- (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 59**

- (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 64**

- (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 67**

- (Exam Topic 2)

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

- A. secondary Smartcenter

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

**Answer:** B

**NEW QUESTION 69**

- (Exam Topic 2)

What is the main difference between Threat Extraction and Threat Emulation?

- A. Threat Emulation never delivers a file and takes more than 3 minutes to complete.
- B. Threat Extraction always delivers a file and takes less than a second to complete.
- C. Threat Emulation never delivers a file that takes less than a second to complete.
- D. Threat Extraction never delivers a file and takes more than 3 minutes to complete.

**Answer:** B

**NEW QUESTION 73**

- (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 76**

- (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 77**

- (Exam Topic 2)

Under which file is the proxy arp configuration stored?

- A. \$FWDIR/state/proxy\_arp.conf on the management server
- B. \$FWDIR/conf/local.arp on the management server
- C. \$FWDIR/state/\_tmp/proxy.arp on the security gateway
- D. \$FWDIR/conf/local.arp on the gateway

**Answer:** D

**NEW QUESTION 80**

- (Exam Topic 2)

What is the purpose of a SmartEvent Correlation Unit?

- A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.
- B. The SmartEvent Correlation Unit's task it to assign severity levels to the identified events.
- C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
- D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.

**Answer:** C

**NEW QUESTION 85**

- (Exam Topic 2)

Which of the following is NOT a type of Check Point API available in R81.x?

- A. Identity Awareness Web Services
- B. OPSEC SDK
- C. Mobile Access
- D. Management

**Answer:** C

**NEW QUESTION 90**

- (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 91

- (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 94

- (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 98

- (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 99

- (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 103

- (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 108

- (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 111**

- (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 114**

- (Exam Topic 2)

What is the most recommended way to install patches and hotfixes?

- A. CPUSE Check Point Update Service Engine
- B. rpm -Uv
- C. Software Update Service
- D. UnixinstallScript

**Answer:** A

**NEW QUESTION 116**

- (Exam Topic 2)

When setting up an externally managed log server, what is one item that will not be configured on the R81 Security Management Server?

- A. IP
- B. SIC
- C. NAT
- D. FQDN

**Answer:** C

**NEW QUESTION 117**

- (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 121**

- (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 123**

- (Exam Topic 2)

SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:

- A. 19090,22
- B. 19190,22
- C. 18190,80
- D. 19009,443

**Answer:** D

**NEW QUESTION 126**

- (Exam Topic 2)

Automation and Orchestration differ in that:

- A. Automation relates to codifying tasks, whereas orchestration relates to codifying processes.
- B. Automation involves the process of coordinating an exchange of information through web service interactions such as XML and JSON, but orchestration does not involve processes.
- C. Orchestration is concerned with executing a single task, whereas automation takes a series of tasks and puts them all together into a process workflow.
- D. Orchestration relates to codifying tasks, whereas automation relates to codifying processes.

**Answer:** A

#### NEW QUESTION 130

- (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 135

- (Exam Topic 2)

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

**Answer:** B

#### NEW QUESTION 137

- (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 140

- (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 141

- (Exam Topic 3)

Which tool is used to enable ClusterXL?

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

**Answer:** B

#### NEW QUESTION 146

- (Exam Topic 3)

The essential means by which state synchronization works to provide failover in the event an active member goes down, \_\_\_\_\_ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

- A. ccp
- B. cphaconf
- C. cphad
- D. cphastart

**Answer:** A

#### NEW QUESTION 147

- (Exam Topic 3)

What is the Implicit Clean-up Rule?

- A. A setting is defined in the Global Properties for all policies.
- B. A setting that is configured per Policy Layer.
- C. Another name for the Clean-up Rule.
- D. Automatically created when the Clean-up Rule is defined.

**Answer:** C

#### NEW QUESTION 152

- (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 155

- (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 158

- (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 159

- (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 161

- (Exam Topic 3)

What command would show the API server status?

- A. cpm status
- B. api restart
- C. api status
- D. show api status

**Answer:** C

#### NEW QUESTION 164

- (Exam Topic 3)

Fill in the blank: The "fw monitor" tool can be best used to troubleshoot \_\_\_\_\_.

- A. AV issues
- B. VPN errors
- C. Network traffic issues
- D. Authentication issues

**Answer:** C

**Explanation:**

[https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit\\_doGoviewsolutiondetails=&solutionid=sk30583](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583)

**NEW QUESTION 166**

- (Exam Topic 3)

Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/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 170**

- (Exam Topic 3)

Capsule Connect and Capsule Workspace both offer secured connection for remote users who are using their mobile devices. However, there are differences between the two.

Which of the following statements correctly identify each product's capabilities?

- A. Workspace supports ios operating system, Android, and WP8, whereas Connect supports ios operating system and Android only
- B. For compliance/host checking, Workspace offers the MDM cooperative enforcement, whereas Connect offers both jailbreak/root detection and MDM cooperative enforcement.
- C. For credential protection, Connect uses One-time Password login support and has no SSO support, whereas Workspace offers both One-Time Password and certain SSO login support.
- D. Workspace can support any application, whereas Connect has a limited number of application types which it will support.

**Answer:** C

**NEW QUESTION 173**

- (Exam Topic 3)

What command lists all interfaces using Multi-Queue?

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

**Answer:** A

**NEW QUESTION 174**

- (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 178**

- (Exam Topic 3)

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

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

**Answer:** A

**NEW QUESTION 183**

- (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 188

- (Exam Topic 3)

In what way are SSL VPN and IPSec VPN different?

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

**Answer:** D

#### NEW QUESTION 192

- (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 195

- (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 200

- (Exam Topic 3)

Which is not a blade option when configuring SmartEvent?

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

**Answer:** B

#### Explanation:

On the Management tab, enable these Software Blades: References:

#### NEW QUESTION 204

- (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 206

- (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 211**

- (Exam Topic 3)

Ken wants to obtain a configuration lock from other administrator on R81 Security Management Server. He can do this via WebUI or via CLI. Which command should he use in CLI? (Choose the correct answer.)

- A. remove database lock
- B. The database feature has one command lock database override.
- C. override database lock
- D. The database feature has two commands lock database override and unlock databas
- E. Both will work.

**Answer:** D

**NEW QUESTION 216**

- (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 217**

- (Exam Topic 3)

You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

- A. sim erdos -e 1
- B. sim erdos - m 1
- C. sim erdos -v 1
- D. sim erdos -x 1

**Answer:** A

**NEW QUESTION 218**

- (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 219**

- (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 221**

- (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 226**

- (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](https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/T)

#### NEW QUESTION 229

- (Exam Topic 4)

Installations and upgrades with CPUSE require that the CPUSE agent is up-to-date. Usually the latest build is downloaded automatically. How can you verify the CPUSE agent build?

- A. In WebUI Status and Actions page or by running the following command in CLISH: show installer status build
- B. In WebUI Status and Actions page or by running the following command in CLISH: show installer status version
- C. In the Management Server or Gateway object in SmartConsole or by running the following command in CLISH: show installer status build
- D. In the Management Server or Gateway object in SmartConsole or by running the following command in CLISH: show installer agent

**Answer:** A

#### NEW QUESTION 230

- (Exam Topic 4)

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

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

**Answer:** C

#### NEW QUESTION 235

- (Exam Topic 4)

Which of the following is NOT a type of Endpoint Identity Agent?

- A. Terminal
- B. Light
- C. Full
- D. Custom

**Answer:** A

#### NEW QUESTION 240

- (Exam Topic 4)

The back end database for Check Point R81 Management uses:

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

**Answer:** C

#### NEW QUESTION 245

- (Exam Topic 4)

D18912E1457D5D1DDCBD40AB3BF70D5D

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

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

**Answer:** B

#### NEW QUESTION 247

- (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 250

- (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 254

- (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 255

- (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 260

- (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 264

- (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 268

- (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 273

- (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 276

- (Exam Topic 4)

How long may verification of one file take for Sandblast Threat Emulation?

- A. up to 1 minutes
- B. within seconds cleaned file will be provided
- C. up to 5 minutes
- D. up to 3 minutes

**Answer:** B

#### NEW QUESTION 281

- (Exam Topic 4)

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

- A. clusterXL\_admin down in Expert Mode
- B. clusterXL\_admin down in Clish
- C. set cluster member state down in Clish
- D. set cluster down in Expert Mode

**Answer:** B

#### NEW QUESTION 285

- (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 288

- (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 290

- (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 293

- (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 294

- (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 299

- (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 304

- (Exam Topic 4)

Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

- A. UserCheck
- B. Active Directory Query
- C. Account Unit Query
- D. User Directory Query

**Answer:** B

#### Explanation:

Reference : [https://sc1.checkpoint.com/documents/R76/CP\\_R76\\_IdentityAwareness\\_AdminGuide/62402.htm](https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm)

#### NEW QUESTION 307

- (Exam Topic 4)

When Identity Awareness is enabled, which identity source(s) is(are) used for Application Control?

- A. RADIUS
- B. Remote Access and RADIUS
- C. AD Query
- D. AD Query and Browser-based Authentication

**Answer:** D

#### Explanation:

Identity Awareness gets identities from these acquisition sources:

#### NEW QUESTION 308

- (Exam Topic 4)

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

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

**Answer:** A

#### NEW QUESTION 313

- (Exam Topic 4)

There are two R77.30 Security Gateways in the Firewall Cluster. They are named FW\_A and FW\_B. The cluster is configured to work as HA (High availability) with default cluster configuration. FW\_A is configured to have higher priority than FW\_B. FW\_A was active and processing the traffic in the morning. FW\_B was standby. Around 1100 am, its interfaces went down and this caused a failover. FW\_B became active. After an hour, FW\_A's interface issues were resolved and it became operational.

When it re-joins the cluster, will it become active automatically?

- A. No, since 'maintain' current active cluster member' option on the cluster object properties is enabled by default.
- B. No, since 'maintain' current active cluster member' option is enabled by default on the Global Properties.
- C. Yes, since 'Switch to higher priority cluster member' option on the cluster object properties is enabled by default.
- D. Yes, since 'Switch to higher priority cluster member' option is enabled by default on the Global Properties.

**Answer:** A

#### NEW QUESTION 315

- (Exam Topic 4)

What is the valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration?

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

**Answer:** B

#### NEW QUESTION 318

- (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 322

- (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 323

- (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 327

- (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 328

- (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 330

- (Exam Topic 4)

Which member of a high-availability cluster should be upgraded first in a Zero downtime upgrade?

- A. The Standby Member

- B. The Active Member
- C. The Primary Member
- D. The Secondary Member

**Answer:** A

#### NEW QUESTION 331

- (Exam Topic 4)

What Is the difference between Updatable Objects and Dynamic Objects

- A. Dynamic Objects are maintained automatically by the Threat Cloud
- B. Updatable Objects are created and maintained locally
- C. In both cases there is no need to install policy for the changes to take effect.
- D. Updatable Objects is a Threat Cloud Service
- E. The provided Objects are updated automatically
- F. Dynamic Objects are created and maintained locally For Dynamic Objectsthere is no need to install policy for the changes to take effect.
- G. Updatable Objects is a Threat Cloud Service
- H. The provided Objects are updated automatically
- I. Dynamic Objects are created and maintained locally In both cases there is no need to install policy for the changes to take effect.
- J. Dynamic Objects are maintained automatically by the Threat Cloud
- K. For Dynamic Objects there is no need to install policy for the changes to take effect
- L. Updatable Objects are created and maintained locally.

**Answer:** B

#### NEW QUESTION 335

- (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 336

- (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 341

- (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 342

- (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 343

- (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 347

- (Exam Topic 4)

What are the available options for downloading Check Point hotfixes in Gala WebUI (CPUSE)?

- A. Manually, Scheduled, Automatic
- B. Manually, Automatic, Disabled
- C. Manually, Scheduled, Disabled
- D. Manually, Scheduled, Enabled

**Answer:** A

#### Explanation:

Reference: [https://sc1.checkpoint.com/documents/R77/CP\\_R77\\_Gaia\\_AdminWebAdminGuide/html\\_frameset.htm?topic=documents/R77/CP\\_R77\\_Gaia\\_AdminWebAdminGuide/112109](https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/112109)

#### NEW QUESTION 348

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

#### NEW QUESTION 349

- (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 350

- (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 351

- (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 352

- (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 node



- 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 node
- F. Use two different Switches to connect both Sync interfaces.
- G. Use a group of bonded interfaces connected to different switches
- 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 356

- (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 359

- (Exam Topic 4)

Aaron is a Cyber 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 mode
- 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 mode
- F. If services are stopped, he should start them with "cpi api start".

**Answer: C**

#### NEW QUESTION 362

- (Exam Topic 4)

What is the correct description for the Dynamic Balancing / Split feature?

- A. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load
- B. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
- C. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's
- D. The interface must support Multi-Queue
- E. It is only available on Quantum Appliances and Open Server (not on Quantum Spark)
- F. Dynamic Balancing / Split dynamically distribute the traffic from one network interface to multiple SND's
- G. The interface must support Multi-Queue
- H. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)
- I. Dynamic Balancing / Split dynamically change the number of SND's and firewall instances based on the current load
- J. It is only available on Quantum Appliances (not on Quantum Spark or Open Server)

**Answer: D**

#### NEW QUESTION 367

- (Exam Topic 4)

What is "Accelerated Policy Installation"?

- A. Starting R81, the Desktop Security Policy installation process is accelerated thereby reducing the duration of the process significantly
- B. Starting R81, the QoS Policy installation process is accelerated thereby reducing the duration of the process significantly
- C. Starting R81, the Access Control Policy installation process is accelerated thereby reducing the duration of the process significantly
- D. Starting R81, the Threat Prevention Policy installation process is accelerated thereby reducing the duration of the process significantly

**Answer: C**

#### NEW QUESTION 371

- (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](https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG)

**NEW QUESTION 372**

- (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 375**

- (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 378**

- (Exam Topic 4)

Check Point ClusterXL Active/Active deployment is used when:

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

**Answer:** D

**NEW QUESTION 381**

.....

## 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](#)**