

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)

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 the SecureXL templates are enabled by default on Security Gateway?

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

Answer: D

NEW QUESTION 3

- (Exam Topic 1)

Which of the following is a new R81 Gateway feature that had not been available in R77.X and older?

- A. The rule base can be built of layers, each containing a set of the security rule
- B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- D. Time object to a rule to make the rule active only during specified times.
- E. Sub Policies are sets of rules that can be created and attached to specific rule
- F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

Which view is NOT a valid CPVIEW view?

- A. IDA
- B. RAD
- C. PDP
- D. VPN

Answer: C

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (Exam Topic 1)

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

- A. The Database revisions will not be synchronized between the management servers
- B. SmartConsole must be closed prior to synchronized changes in the objects database
- C. If you wanted to use Full Connectivity Upgrade, you must change the Implied Rules to allow FW1_cpersistent to pass before the Firewall Control Connections.
- D. For Management Server synchronization, only External Virtual Switches are supported
- E. So, if you wanted to employ Virtual Routers instead, you have to reconsider your design.

Answer: A

NEW QUESTION 9

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 10

- (Exam Topic 1)

Which command can you use to enable or disable multi-queue per interface?

- A. cpmq set
- B. Cpmqueue set
- C. Cpmq config
- D. St cpmq enable

Answer: A

NEW QUESTION 10

- (Exam Topic 1)

Which CLI command will reset the IPS pattern matcher statistics?

- A. ips reset pmstat
- B. ips pstats reset
- C. ips pmstats refresh
- D. ips pmstats reset

Answer: D

NEW QUESTION 12

- (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 16

- (Exam Topic 1)

The Firewall kernel is replicated multiple times, therefore:

- A. The Firewall kernel only touches the packet if the connection is accelerated
- B. The Firewall can run different policies per core

- C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
- D. The Firewall can run the same policy on all cores.

Answer: D

Explanation:

On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.

NEW QUESTION 18

- (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 20

- (Exam Topic 1)

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

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

Answer: C

Explanation:

Suspicious Activity Rules Solution

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

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

NEW QUESTION 22

- (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 24

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 26

- (Exam Topic 1)

You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

- A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules.
- B. Create a separate Security Policy package for each remote Security Gateway.
- C. Create network objects that restricts all applicable rules to only certain networks.
- D. Run separate SmartConsole instances to login and configure each Security Gateway directly.

Answer: B

NEW QUESTION 31

- (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 34

- (Exam Topic 1)

Selecting an event displays its configurable properties in the Detail pane and a description of the event in the Description pane. Which is NOT an option to adjust or configure?

- A. Severity
- B. Automatic reactions
- C. Policy
- D. Threshold

Answer: C

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 40

- (Exam Topic 1)

When requiring certificates for mobile devices, make sure the authentication method is set to one of the following, Username and Password, RADIUS or _____.

- A. SecureID
- B. SecurID
- C. Complexity
- D. TacAcs

Answer: B

NEW QUESTION 43

- (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 44

- (Exam Topic 1)

Which of the following process pulls application monitoring status?

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

Answer: D

NEW QUESTION 46

- (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 47

- (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 51

- (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 52

- (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 54

- (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 57

- (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 61

- (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 63

- (Exam Topic 1)

The Event List within the Event tab contains:

- A. a list of options available for running a query.
- B. the top events, destinations, sources, and users of the query results, either as a chart or in a tallied list.
- C. events generated by a query.
- D. the details of a selected event.

Answer: C

NEW QUESTION 68

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 71

- (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 73

- (Exam Topic 1)

What is the correct command to observe the Sync traffic in a VRRP environment?

- A. `fw monitor -e "accept[12:4,b]=224.0.0.18;"`
- B. `fw monitor -e "accept port(6118;"`
- C. `fw monitor -e "accept proto=mcVRRP;"`
- D. `fw monitor -e "accept dst=224.0.0.18;"`

Answer: D

NEW QUESTION 74

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 79

- (Exam Topic 1)

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 83

- (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 87

- (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 88

- (Exam Topic 1)

What command verifies that the API server is responding?

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

Answer: B

NEW QUESTION 91

- (Exam Topic 1)

What is true about VRRP implementations?

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

Answer: C

NEW QUESTION 92

- (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 97

- (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 99

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 102

- (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 107

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 112

- (Exam Topic 2)

Which GUI client is supported in R81?

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

Answer: C

NEW QUESTION 114

- (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 119

- (Exam Topic 2)

You need to see which hotfixes are installed on your gateway, which command would you use?

- A. cpinfo -h all
- B. cpinfo -o hotfix
- C. cpinfo -l hotfix
- D. cpinfo -y all

Answer: D

NEW QUESTION 122

- (Exam Topic 2)

As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

- A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
- B. Full Layer4 VPN –SSL VPN that gives users network access to all mobile applications.
- C. Full Layer3 VPN –IPSec VPN that gives users network access to all mobile applications.
- D. You can make sure that documents are sent to the intended recipients only.

Answer: C

NEW QUESTION 123

- (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 124

- (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 128

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 131

- (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 134

- (Exam Topic 2)

SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

- A. Threat Emulation
- B. Mobile Access
- C. Mail Transfer Agent
- D. Threat Cloud

Answer: B

NEW QUESTION 139

- (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 142

- (Exam Topic 2)

Which Check Point daemon monitors the other daemons?

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

Answer: C

NEW QUESTION 144

- (Exam Topic 2)

The Correlation Unit performs all but the following actions:

- A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.
- B. Generates an event based on the Event policy.
- C. Assigns a severity level to the event.
- D. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event.

Answer: C

NEW QUESTION 149

- (Exam Topic 2)
What processes does CPM control?

- A. Object-Store, Database changes, CPM Process and web-services
- B. web-services, CPMI process, DLEserver, CPM process
- C. DLEServer, Object-Store, CP Process and database changes
- D. web_services, dle_server and object_Store

Answer: D

NEW QUESTION 153

- (Exam Topic 2)
What are the main stages of a policy installations?

- A. Verification & Compilation, Transfer and Commit
- B. Verification & Compilation, Transfer and Installation
- C. Verification, Commit, Installation
- D. Verification, Compilation & Transfer, Installation

Answer: A

NEW QUESTION 157

- (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 160

- (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 165

- (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 166

- (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 170

- (Exam Topic 2)
What API command below creates a new host with the name "New Host" and IP address of "192.168.0.10"?

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

Answer: D

NEW QUESTION 172

- (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 174

- (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 178

- (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 181

- (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 185

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 187

- (Exam Topic 2)

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

- A. For short connections like http service – delay sync for 2 seconds
- 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 192

- (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 194

- (Exam Topic 2)

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

- A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
- B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
- C. Mail, Block Source, Block Destination, External Script, SNMP Trap
- D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

NEW QUESTION 199

- (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 200

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 205

- (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 Policy
- 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 207

- (Exam Topic 2)

What component of R81 Management is used for indexing?

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

Answer: D

NEW QUESTION 209

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 210

- (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 215

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 218

- (Exam Topic 2)

SandBlast appliances can be deployed in the following modes:

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

Answer: C

NEW QUESTION 221

- (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 224

- (Exam Topic 3)

In what way is Secure Network Distributor (SND) a relevant feature of the Security Gateway?

- A. SND is a feature to accelerate multiple SSL VPN connections
- B. SND is an alternative to IPSec Main Mode, using only 3 packets
- C. SND is used to distribute packets among Firewall instances
- D. SND is a feature of fw monitor to capture accelerated packets

Answer: C

NEW QUESTION 229

- (Exam Topic 3)

Which Check Point software blade provides Application Security and identity control?

- A. Identity Awareness
- B. Data Loss Prevention
- C. URL Filtering
- D. Application Control

Answer: D

NEW QUESTION 234

- (Exam Topic 3)

What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 235

- (Exam Topic 3)

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

- A. Next Generation Threat Prevention
- B. Next Generation Threat Emulation
- C. Next Generation Threat Extraction
- D. Next Generation Firewall

Answer: B

NEW QUESTION 240

- (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 243

- (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 244

- (Exam Topic 3)

You have a Geo-Protection policy blocking Australia and a number of other countries. Your network now requires a Check Point Firewall to be installed in Sydney, Australia.

What must you do to get SIC to work?

- A. Remove Geo-Protection, as the IP-to-country database is updated externally, and you have no control of this.
- B. Create a rule at the top in the Sydney firewall to allow control traffic from your network
- C. Nothing - Check Point control connections function regardless of Geo-Protection policy
- D. Create a rule at the top in your Check Point firewall to bypass the Geo-Protection

Answer: C

NEW QUESTION 249

- (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 250

- (Exam Topic 3)

To ensure that VMAC mode is enabled, which CLI command should you run on all cluster members?

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

Answer: D

NEW QUESTION 251

- (Exam Topic 3)

You have a Gateway is running with 2 cores. You plan to add a second gateway to build a cluster and used a device with 4 cores. How many cores can be used in a Cluster for Firewall-kernel on the new device?

- A. 3
- B. 2

- C. 1
- D. 4

Answer: D

NEW QUESTION 256

- (Exam Topic 3)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 261

- (Exam Topic 3)

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

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

Answer: D

NEW QUESTION 266

- (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 270

- (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 272

- (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 275

- (Exam Topic 3)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 279

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 283

- (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 285

- (Exam Topic 3)

Fill in the blank. Once a certificate is revoked from the Security Gateway by the Security Management Server, the certificate information is _____ .

- A. Sent to the Internal Certificate Authority.
- B. Sent to the Security Administrator.
- C. Stored on the Security Management Server.
- D. Stored on the Certificate Revocation List.

Answer: D

NEW QUESTION 290

- (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 291

- (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 293

- (Exam Topic 3)

Office mode means that:

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

Answer: D

NEW QUESTION 298

- (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 301

- (Exam Topic 3)

Which of the following technologies extracts detailed information from packets and stores that information in state tables?

- A. INSPECT Engine
- B. Stateful Inspection
- C. Packet Filtering
- D. Application Layer Firewall

Answer: A

NEW QUESTION 304

- (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 306

- (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 308

- (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 309

- (Exam Topic 3)

Which application should you use to install a contract file?

- A. SmartView Monitor
- B. WebUI
- C. SmartUpdate
- D. SmartProvisioning

Answer: C

NEW QUESTION 313

- (Exam Topic 3)

Which of the following commands shows the status of processes?

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

Answer: D

NEW QUESTION 317

- (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 318

- (Exam Topic 3)

The SmartEvent R81 Web application for real-time event monitoring is called:

- A. SmartView Monitor
- B. SmartEventWeb
- C. There is no Web application for SmartEvent
- D. SmartView

Answer: B

NEW QUESTION 323

- (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 327

- (Exam Topic 3)

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CPApp

Answer: B

NEW QUESTION 328

- (Exam Topic 3)

During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

- A. Dropped without sending a negative acknowledgment
- B. Dropped without logs and without sending a negative acknowledgment
- C. Dropped with negative acknowledgment
- D. Dropped with logs and without sending a negative acknowledgment

Answer: D

NEW QUESTION 329

- (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 333

- (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 334

- (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 339

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 343

- (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 348

- (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 350

- (Exam Topic 3)

In ClusterXL Load Sharing Multicast Mode:

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

Answer: D

NEW QUESTION 353

- (Exam Topic 3)

What is the responsibility of SOLR process on R81.10 management server?

- A. Validating all data before it's written into the database
- B. It generates indexes of data written to the database
- C. Communication between SmartConsole applications and the Security Management Server
- D. Writing all information into the database

Answer: B

NEW QUESTION 357

- (Exam Topic 3)

How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 361

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 364

- (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 369

- (Exam Topic 3)

What are the methods of SandBlast Threat Emulation deployment?

- A. Cloud, Appliance and Private
- B. Cloud, Appliance and Hybrid
- C. Cloud, Smart-1 and Hybrid
- D. Cloud, OpenServer and VMware

Answer: A

NEW QUESTION 370

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 374

- (Exam Topic 3)

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

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

Answer: A

NEW QUESTION 378

- (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 382

- (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 383

- (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 385

- (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 of 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 387

- (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 388

- (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 389

- (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 390

- (Exam Topic 4)

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

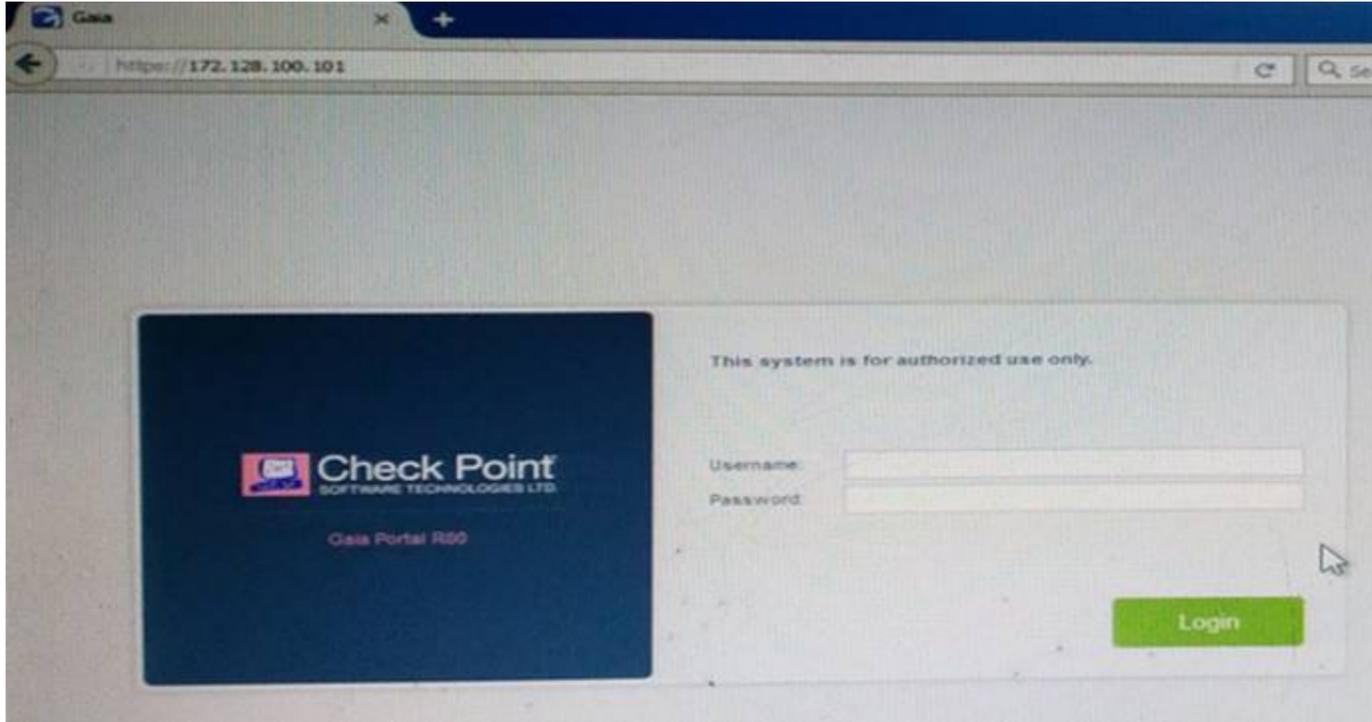
- A. run fw unloadlocal" on the relevant gateway and check the ping again
- B. run "cpstop" on the relevant gateway and check the ping again
- C. run "fw log" on the relevant gateway
- D. run "fw ctl zdebug drop" on the relevant gateway

Answer: D

NEW QUESTION 393

- (Exam Topic 4)

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



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

Answer: A

NEW QUESTION 397

- (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 398

- (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 403

- (Exam Topic 4)

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

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

Answer: A

Explanation:

Types of Solutions

All of Check Point's Remote Access solutions provide:

NEW QUESTION 405

- (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 408

- (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 410

- (Exam Topic 4)

True or False: In a Distributed Environment, a Central License can be installed via CLI on a Security Gateway.

- A. True, CLI is the prefer method for Licensing
- B. False, Central License are handled via Security Management Server
- C. False, Central Licenses are installed via Gaia on Security Gateways
- D. True, Central License can be installed with CPLIC command on a Security Gateway

Answer: D

NEW QUESTION 413

- (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 417

- (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 420

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 423

- (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 425

- (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 429

- (Exam Topic 4)

Fill in the blank: A _____ VPN deployment is used to provide remote users with secure access to internal corporate resources by authenticating the user through an internet browser.

- A. Clientless remote access
- B. Clientless direct access
- C. Client-based remote access
- D. Direct access

Answer: A

NEW QUESTION 431

- (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 432

- (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 435

- (Exam Topic 4)

Which of the following is NOT a valid type of SecureXL template?

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

Answer: B

NEW QUESTION 437

- (Exam Topic 4)

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

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

Answer: B

Explanation:

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

NEW QUESTION 441

- (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 443

- (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 445

- (Exam Topic 4)

Which upgrade method you should use upgrading from R80.40 to R81.10 to avoid any downtime?

- A. Zero Downtime Upgrade (ZDU)
- B. Connectivity Upgrade (CU)
- C. Minimal Effort Upgrade (ME)
- D. Multi-Version Cluster Upgrade (MVC)

Answer: D

NEW QUESTION 447

- (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 449

- (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 450

- (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 454

- (Exam Topic 4)

What traffic does the Anti-bot feature block?

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

Answer: A

NEW QUESTION 459

- (Exam Topic 4)

Which command will reset the kernel debug options to default settings?

- A. fw ctl dbg -a 0
- B. fw ctl dbg resetall
- C. fw ctl debug 0
- D. fw ctl debug set 0

Answer: C

NEW QUESTION 464

- (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 SmartConsole
- 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 SmartConsole
- 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 SmartConsole
- 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 SmartConsole
- 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 ttcpahaconf 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 466

- (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 468

- (Exam Topic 4)

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

- A. Go to clash-Run cpstop | Run cpstart
- B. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway
- C. Administrator does not need to perform any tas
- D. Check Point will make use of the newly installed CPU and Cores
- E. Go to clash-Run cpconfig | Configure CoreXL to make use of the additional Cores | Exit cpconfig | Reboot Security Gateway | Install Security Policy

Answer: B

NEW QUESTION 472

- (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 475

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 480

- (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 485

- (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 488

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 490

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 492

- (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 497

- (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 500

- (Exam Topic 4)

Which process handles connection from SmartConsole R81?

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

Answer: C

NEW QUESTION 502

- (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 503

- (Exam Topic 4)

On R81.10 the IPS Blade is managed by:

- A. Threat Protection policy
- B. Anti-Bot Blade
- C. Threat Prevention policy
- D. Layers on Firewall policy

Answer: C

NEW QUESTION 505

- (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 507

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 509

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 512

- (Exam Topic 4)

What is the best sync method in the ClusterXL deployment?

- A. Use 1 cluster + 1st sync
- B. Use 1 dedicated sync interface
- C. Use 3 clusters + 1st sync + 2nd sync + 3rd sync
- D. Use 2 clusters + 1st sync + 2nd sync

Answer: B

NEW QUESTION 513

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 518

- (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 520

- (Exam Topic 4)

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

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

Answer: A

Explanation:

https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_PerformanceTuning_AdminG_R81

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

NEW QUESTION 522

- (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 524

- (Exam Topic 4)

What is the correct order of the default "fw monitor" inspection points?

- A. i, l, o, O
- B. 1, 2, 3, 4
- C. i, o, l, O
- D. l, i, O, o

Answer: C

NEW QUESTION 526

- (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 529

- (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 530

- (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 534

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 535

- (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 536

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 541

- (Exam Topic 4)

What is the purpose of the CPCA process?

- A. Monitoring the status of processes.
- B. Sending and receiving logs.
- C. Communication between GUI clients and the SmartCenter server.
- D. Generating and modifying certificates.

Answer: D

NEW QUESTION 542

- (Exam Topic 4)

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

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

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

Answer: A

NEW QUESTION 546

- (Exam Topic 4)

What is false regarding a Management HA environment?

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

Answer: B

NEW QUESTION 549

- (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 551

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 556

- (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 558

- (Exam Topic 4)

How is communication between different Check Point components secured in R81? As with all questions, select the BEST answer.

- A. By using IPSEC
- B. By using SIC

- C. By using ICA
- D. By using 3DES

Answer: B

NEW QUESTION 560

- (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 562

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 564

- (Exam Topic 4)

What is the benefit of Manual NAT over Automatic NAT?

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

Answer: C

NEW QUESTION 567

- (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 568

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 569

- (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 570

- (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 573

- (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 574

- (Exam Topic 4)

SmartEvent Security Checkups can be run from the following Logs and Monitor activity:

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

Answer: A

NEW QUESTION 576

- (Exam Topic 4)

Main Mode in IKEv1 uses how many packages for negotiation?

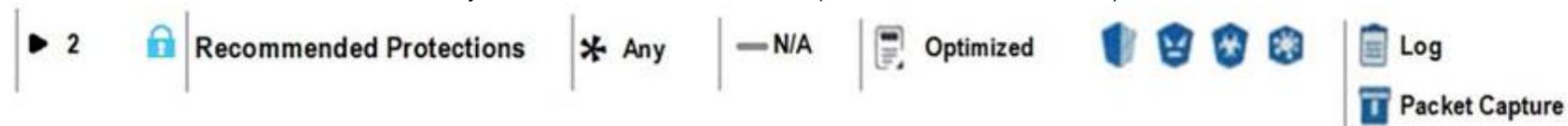
- A. 4
- B. depends on the make of the peer gateway
- C. 3
- D. 6

Answer: C

NEW QUESTION 579

- (Exam Topic 4)

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



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

Answer: B

Explanation:

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

NEW QUESTION 583

- (Exam Topic 4)

What two ordered layers make up the Access Control Policy Layer?

- A. URL Filtering and Network
- B. Network and Threat Prevention
- C. Application Control and URL Filtering
- D. Network and Application Control

Answer: D

NEW QUESTION 585

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 586

- (Exam Topic 4)

What component of Management is used for indexing?

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

Answer: D

Explanation:

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

NEW QUESTION 589

- (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 591

- (Exam Topic 4)

Which of the following processes pulls the application monitoring status from gateways?

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

Answer: A

NEW QUESTION 592

- (Exam Topic 4)

Mobile Access Gateway can be configured as a reverse proxy for Internal Web Applications Reverse proxy users browse to a URL that is resolved to the Security Gateway IP address. Which of the following Check Point command is true for enabling the Reverse Proxy:

- A. ReverseCLIProxy
- B. ReverseProxyCLI
- C. ReverseProxy
- D. ProxyReverseCLI

Answer: C

NEW QUESTION 594

- (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 596

- (Exam Topic 4)

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

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

Answer: C

Explanation:

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

NEW QUESTION 600

- (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 603

- (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 606

- (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 611

- (Exam Topic 4)

IF the first packet of an UDP session is rejected by a rule definition from within a security policy (not including the clean up rule), what message is sent back through the kernel?

- A. Nothing
- B. TCP FIN
- C. TCP RST
- D. ICMP unreachable

Answer: A

NEW QUESTION 616

- (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 619

- (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 623

- (Exam Topic 4)

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

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

Answer: B

NEW QUESTION 627

- (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 630

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 633

- (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 637

- (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 640

- (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 642

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 646

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 651

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 655

- (Exam Topic 4)

In the Check Point Security Management Architecture, which component(s) can store logs?

- A. SmartConsole
- B. Security Management Server and Security Gateway
- C. Security Management Server
- D. SmartConsole and Security Management Server

Answer: B

NEW QUESTION 658

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 659

- (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 662

- (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 665

- (Exam Topic 4)

Which command shows the current Security Gateway Firewall chain?

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

Answer: C

NEW QUESTION 669

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 670

- (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 672

.....

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