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

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

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
How can SmartView application accessed?

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

Answer: C

NEW QUESTION 5
- (Exam Topic 1)
What has to be taken into consideration when configuring Management HA?

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

Answer: A

NEW QUESTION 6
- (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 7
- (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 8
- (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 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)
Fill in the blank: The tool _____ generates a R81 Security Gateway configuration report.

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

Answer: C

NEW QUESTION 10
- (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 13
- (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)
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 22
- (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 26
- (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 27
- (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 28
- (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 30
- (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 31
- (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 32
- (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 35
- (Exam Topic 1)
In a Client to Server scenario, which inspection point is the first point immediately following the tables and rule base check of a packet coming from outside of the network?

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

Answer: A

NEW QUESTION 38
- (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 39
- (Exam Topic 1)
Where you can see and search records of action done by R81 SmartConsole administrators?

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

Answer: B

NEW QUESTION 43
- (Exam Topic 1)
Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

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

Answer: D

NEW QUESTION 48
- (Exam Topic 1)
What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 49
- (Exam Topic 1)
To fully enable Dynamic Dispatcher on a Security Gateway:

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

Answer: A

NEW QUESTION 54
- (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 56
- (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 59
- (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 62
- (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 64
- (Exam Topic 2)
What is the purpose of extended master key extension/session hash?

A. UDP VOIP protocol extension
B. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-server communication
C. Special TCP handshaking extension
D. Supplement DLP data watermark

Answer: B

NEW QUESTION 65
- (Exam Topic 2)
In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with _____ will not apply.

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

Answer: B

NEW QUESTION 67
- (Exam Topic 2)
Which configuration file contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status?

A. $FWDIR/database/fwauthd.conf
B. $FWDIR/conf/fwauth.conf

C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/state/fwauthd.conf

Answer: C

NEW QUESTION 69
- (Exam Topic 2)
Which encryption algorithm is the least secured?

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

Answer: C

NEW QUESTION 74
- (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 79
- (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 82
- (Exam Topic 2)
Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs
B. Capsule Cloud
C. Capsule Enterprise
D. Capsule Workspace

Answer: C

NEW QUESTION 87
- (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 92
- (Exam Topic 2)
SmartEvent does NOT use which of the following procedures to identify events:

A. Matching a log against each event definition
B. Create an event candidate
C. Matching a log against local exclusions
D. Matching a log against global exclusions

Answer: C

Explanation:
Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:
• Matching a Log Against Global Exclusions
• Matching a Log Against Each Event Definition

• Creating an Event Candidate
• When a Candidate Becomes an Event References:

NEW QUESTION 93
- (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 94
- (Exam Topic 2)
With Mobile Access enabled, administrators select the web-based and native applications that can be accessed by remote users and define the actions that users can perform the applications. Mobile Access encrypts all traffic using:

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

Answer: A

NEW QUESTION 98
- (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 101
- (Exam Topic 2)
What is considered Hybrid Emulation Mode?

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

Answer: B

NEW QUESTION 102
- (Exam Topic 2)
Using ClusterXL, what statement is true about the Sticky Decision Function?

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

Answer: A

NEW QUESTION 105
- (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 108
- (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 112
- (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 113
- (Exam Topic 3)
What cloud-based SandBlast Mobile application is used to register new devices and users?

A. Check Point Protect Application
B. Management Dashboard
C. Behavior Risk Engine
D. Check Point Gateway

Answer: D

NEW QUESTION 117
- (Exam Topic 3)
When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

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

Answer: D

NEW QUESTION 121
- (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 125
- (Exam Topic 3)
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 128
- (Exam Topic 3)
What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 131
- (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 132
- (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 135
- (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 138
- (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 139
- (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 143
- (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 148
- (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 151
- (Exam Topic 3)
Office mode means that:

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

Answer: D

NEW QUESTION 156
- (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 160
- (Exam Topic 3)
What kind of information would you expect to see using the sim affinity command?

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

Answer: D

NEW QUESTION 165
- (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 166
- (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 169
- (Exam Topic 3)
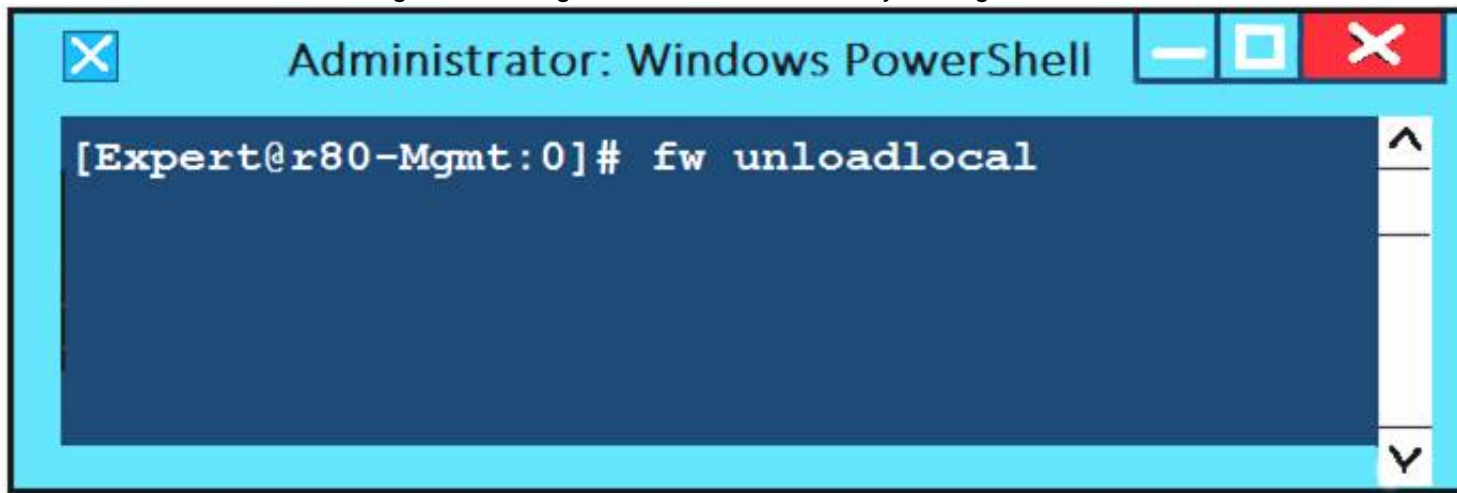In the Firewall chain mode FFF refers to:

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

Answer: C

NEW QUESTION 174
- (Exam Topic 3)
What will be the effect of running the following command on the Security Management Server?

```
[Expert@r80-Mgmt:0]# fw unloadlocal
```

A. Remove the installed Security Policy.
B. Remove the local ACL lists.
C. No effect.
D. Reset SIC on all gateways.

Answer: A

NEW QUESTION 175
- (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 179
- (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 181
- (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 186
- (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 Kernal, 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 190
- (Exam Topic 3)
What does it mean if Deyra sees the gateway status? (Choose the BEST answer.)

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

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

Answer: B

NEW QUESTION 195
- (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 199
- (Exam Topic 4)
Alice knows about the Check Point Management HA installation from Bob and needs to know which Check Point Security Management Server is currently capable of issuing and managing certificate. Alice uses the Check Point command "cpconfig" to run the Check Point Security Management Server configuration tool on both Check Point Management HA instances "Primary & Secondary" Which configuration option does she need to look for:

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

Answer: D

NEW QUESTION 204
- (Exam Topic 4)
Which Check Point daemon invokes and monitors critical processes and attempts to restart them if they fail?

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

Answer: C

NEW QUESTION 205
- (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?
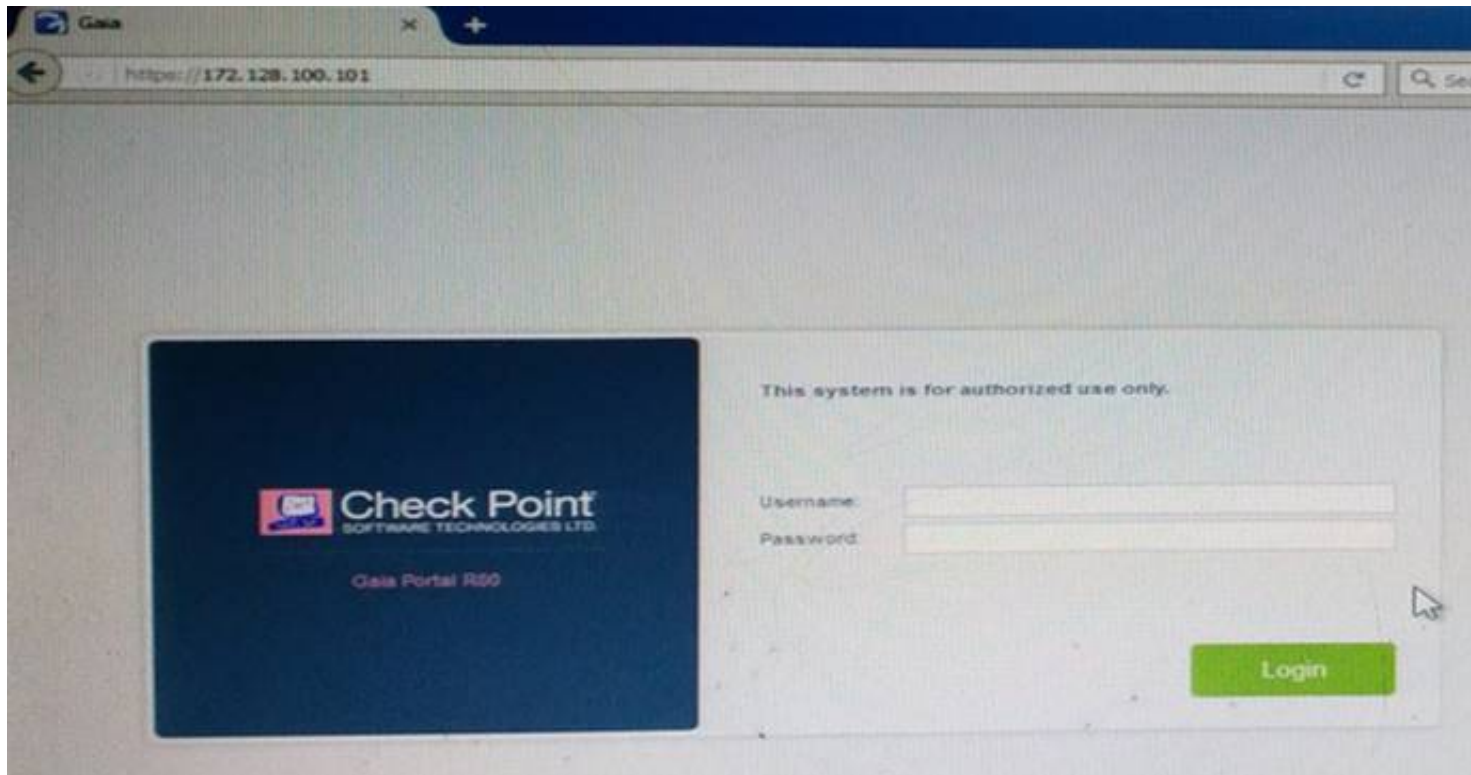
A. run fw unloadlocal'' on the relevant gateway and check the ping again
B. run "cpstop" on the relevant gateway and check the ping again
C. run ''fw log" on the relevant gateway
D. run ''fw ctl zdebug drop" on the relevant gateway

Answer: D

NEW QUESTION 208
- (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 210
- (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 212
- (Exam Topic 4)
Bob works for a big security outsourcing provider company and as he receives a lot of change requests per day he wants to use for scripting daily tasks the API services (torn Check Point for the GAIA API. Firstly he needs to be aware if the API services are running for iheGAIA operating system. Which of the following Check Point Command is true:

A. gala_dlish status
B. status gaiaapi
C. api_gala status
D. gala_api status

Answer: A

NEW QUESTION 216
- (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 218
- (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 223
- (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 226
- (Exam Topic 4)
Choose the correct syntax to add a new host named "emailserver1" with IP address 10.50.23.90 using GAiA Management CLI?

A. mgmt_cli add host name "myHost12 ip" address 10.50.23.90
B. mgmt_cli add host name ip-address 10.50.23.90
C. mgmt_cli add host "emailserver1" address 10.50.23.90
D. mgmt_cli add host name "emailserver1" ip-address 10.50.23.90

Answer: D

Explanation:
Reference: https://weekly-geekly.github.io/articles/339924/index.html

NEW QUESTION 229
- (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 232
- (Exam Topic 4)
Which Queue in the Priority Queue has the maximum priority?

A. High Priority
B. Control
C. Routing
D. Heavy Data Queue

Answer: C

NEW QUESTION 235
- (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 238
- (Exam Topic 4)
What is required for a site-to-site VPN tunnel that does not use certificates?

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

Answer: A

NEW QUESTION 239
- (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 241
- (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 246
- (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 249
- (Exam Topic 4)
You had setup the VPN Community VPN-Stores'with 3 gateways. There are some issues with one remote gateway(1.1.1.1) and an your local gateway. What will be the best log filter to see only the IKE Phase 2 agreed networks for both gateways

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

Answer: C

NEW QUESTION 250
- (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 252
- (Exam Topic 4)
You need to change the MAC-address on eth2 interface of the gateway. What is the correct way to change MAC-address in Check Point Gaia?

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

Answer: A

NEW QUESTION 255
- (Exam Topic 4)
An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret and cannot be enabled. Why does it not allow him to specify the pre-shared secret?

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

Answer: C

NEW QUESTION 257
- (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 262
- (Exam Topic 4)
Which TCP port does the CPM process listen on?

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

Answer: D

NEW QUESTION 265
- (Exam Topic 4)
SecureXL is able to accelerate the Connection Rate using templates. Which attnbutes are used in the template to identify the connection?

A. Source address . Destination addres
B. Source Port, Destination port
C. Source address . Destination addres
D. Destination port
E. Source address . Destination addres
F. Destination por
G. Pro^col
H. Source address . Destination addres
I. Source Port, Destination por
J. Protocol

Answer: D

NEW QUESTION 268
- (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 273
- (Exam Topic 4)

No.	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
1	NetBIOS Noise	✳ Any	✳ Any	✳ Any	⌘ NBT	🔴 Drop	— None	✳ Policy Targets
2	Management	⛢ Net_10.28.0.0	▭ GW-R.7730	✳ Any	🌐 https ⚡ ssh	🟢 Accept	📄 Log	✳ Policy Targets
3	Stealth	✳ Any	▭ GW-R.7730	✳ Any	✳ Any	🔴 Drop	📄 Log	✳ Policy Targets
4	DNS	⛢ Net_10.28.0.0	✳ Any	✳ Any	⌘ dns	🟢 Accept	📄 Log	✳ Policy Targets
5	Web	⛢ Net_10.28.0.0	✳ Any	✳ Any	🌐 http 🌐 https	🟢 Accept	📄 Log	✳ Policy Targets
6	✎ DMZ Access	⛢ Net_10.28.0.0	⛢ DMZ_Net_192.0.2.0	✳ Any	🔵 ftp ⚡ AP-Defender	🟢 Accept	📄 Log	✳ Policy Targets
7	Cleanup rule	✳ Any	✳ Any	✳ Any	✳ Any	🔴 Drop	📄 Log	✳ Policy Targets

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

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

Answer: C

NEW QUESTION 277
- (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 282
- (Exam Topic 4)
In the R81 SmartConsole, on which tab are Permissions and Administrators defined?

A. Security Policies
B. Logs and Monitor
C. Manage and Settings
D. Gateways and Servers

Answer: C

NEW QUESTION 286
- (Exam Topic 4)
Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new multicore CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

A. 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 287
- (Exam Topic 4)
If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

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

Answer: D

NEW QUESTION 288
- (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 289
- (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 291
- (Exam Topic 4)
When detected, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure one Automatic Reaction, or many, according to the needs of the system. Which of the following statement is false and NOT part of possible automatic reactions:

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

Answer: B

NEW QUESTION 293
- (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 296
- (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 300
- (Exam Topic 4)
What level of CPU load on a Secure Network Distributor would indicate that another may be necessary?

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

Answer: A

NEW QUESTION 302
- (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 306
- (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 309
- (Exam Topic 4)
The admin lost access to the Gaia Web Management Interface but he was able to connect via ssh. How can you check if the web service is enabled, running and which port is used?

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

Answer: C

NEW QUESTION 311
- (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 312
- (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 315
- (Exam Topic 4)
SmartEvent Security Checkups can be run from the following Logs and Monitor activity:
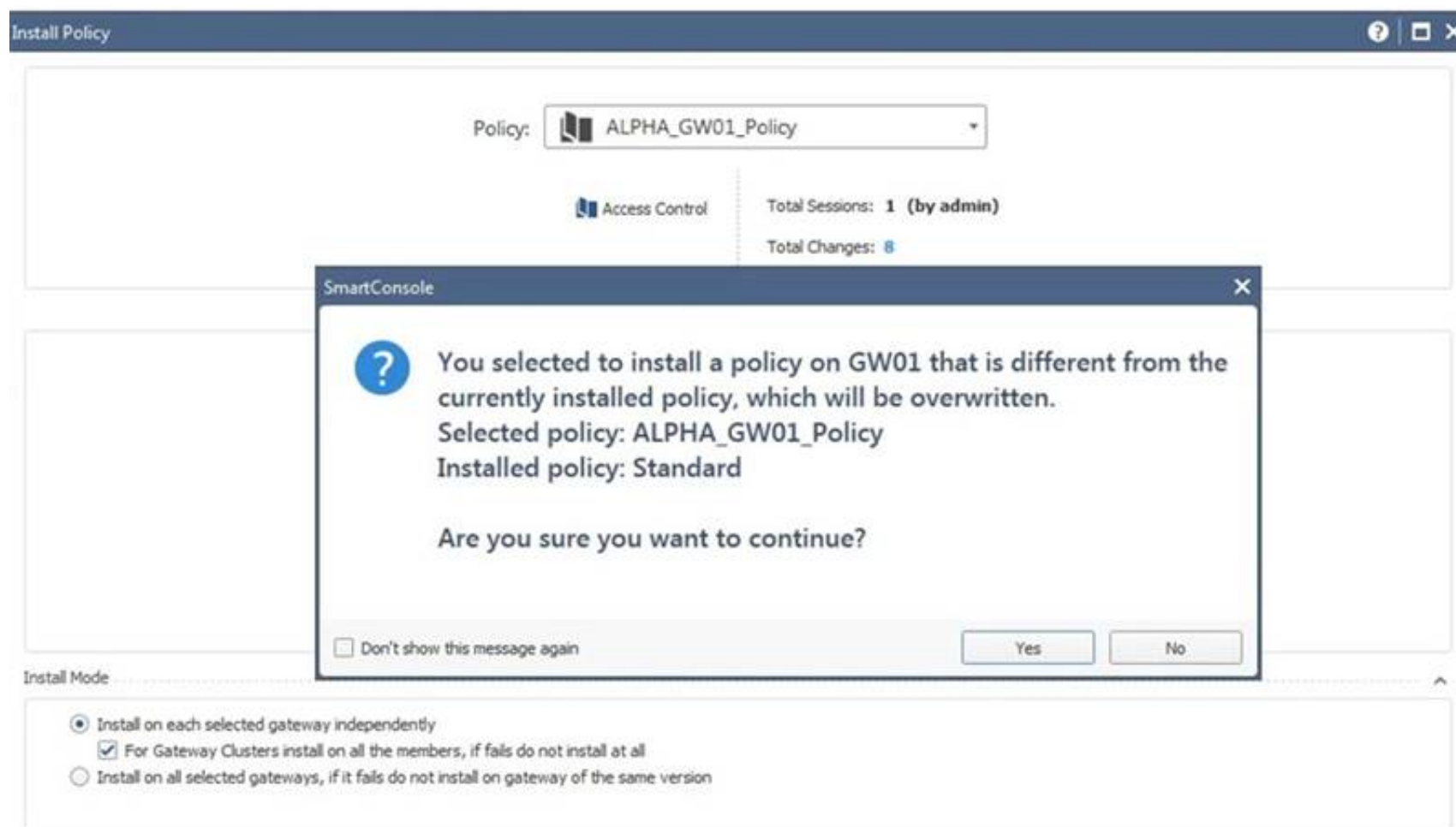
A. Reports
B. Advanced
C. Checkups
D. Views

Answer: A

NEW QUESTION 316
- (Exam Topic 4)
Why would an administrator see the message below?

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

Answer: B

NEW QUESTION 318
- (Exam Topic 4)
What is false regarding prerequisites for the Central Deployment usage?

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

Answer: D

NEW QUESTION 322
- (Exam Topic 4)
An established connection is going to www.google.com. The Application Control Blade Is inspecting the traffic. If SecureXL and CoreXL are both enabled, which path is handling the traffic?

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

Answer: D

NEW QUESTION 323
- (Exam Topic 4)
Which Check Point process provides logging services, such as forwarding logs from Gateway to Log Server, providing Log Export API (LEA) & Event Logging API (EL-A) services.

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

Answer: A

NEW QUESTION 328
- (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 329
- (Exam Topic 4)
When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Answer: C

NEW QUESTION 330
- (Exam Topic 4)
Which Check Point software blade provides protection from zero-day and undiscovered threats?

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

Answer: B

NEW QUESTION 334
- (Exam Topic 4)
What are the two modes for SNX (SSL Network Extender)?

A. Network Mode and Application Mode
B. Visitor Mode and Office Mode
C. Network Mode and Hub Mode
D. Office Mode and Hub Mode

Answer: A

NEW QUESTION 339
- (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 343
- (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 345
- (Exam Topic 4)
Fill in the blank: _____ information is included in "Full Log" tracking option, but is not included in "Log" tracking option?

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

Answer: B

NEW QUESTION 349
- (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 351
......

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