CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

About Exambible

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

　　All examinations will be up to date.

* 24/7 Quality Support

　　We will provide service round the clock.

* 100% Pass Rate

　　Our guarantee that you will pass the exam.

* Unique Gurantee

　　If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 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 ae 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 3
- (Exam Topic 1)
Which of these statements describes the Check Point ThreatCloud?

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

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
fwssd is a child process of which of the following Check Point daemons?

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

Answer: A

NEW QUESTION 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 is used to set the CCP protocol to Multicast?

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

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

A. 15 sec
B. 60 sec
C. 5 sec
D. 30 sec

Answer: B

NEW QUESTION 8
- (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 9
- (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 10
- (Exam Topic 1)
Fill in the blank: The command _____ provides the most complete restoration of a R81 configuration.

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

Answer: A

NEW QUESTION 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 11
- (Exam Topic 1)
Which command will allow you to see the interface status?

A. cphaprob interface
B. cphaprob –I interface
C. cphaprob –a if
D. cphaprob stat

Answer: C

NEW QUESTION 14
- (Exam Topic 1)
Advanced Security Checkups can be easily conducted within:

A. Reports
B. Advanced
C. Checkups
D. Views
E. Summary

Answer: A

NEW QUESTION 18
- (Exam Topic 1)
The Firewall Administrator is required to create 100 new host objects with different IP addresses. What API command can he use in the script to achieve the requirement?

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

Answer: A

NEW QUESTION 23
- (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 26
- (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 27
- (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 32
- (Exam Topic 1)
To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab.
How many options are available to calculate the traffic direction?

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

Answer: D

NEW QUESTION 35
- (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 38
- (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 43
- (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 48
- (Exam Topic 1)
In R81, how do you manage your Mobile Access Policy?

A. Through the Unified Policy
B. Through the Mobile Console
C. From SmartDashboard
D. From the Dedicated Mobility Tab

Answer: A

NEW QUESTION 50
- (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 53
- (Exam Topic 1)
Session unique identifiers are passed to the web api using which http header option?

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

Answer: C

NEW QUESTION 58
- (Exam Topic 1)
What are the three components for Check Point Capsule?

A. Capsule Docs, Capsule Cloud, Capsule Connect
B. Capsule Workspace, Capsule Cloud, Capsule Connect
C. Capsule Workspace, Capsule Docs, Capsule Connect
D. Capsule Workspace, Capsule Docs, Capsule Cloud

Answer: D

NEW QUESTION 61
- (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 65
- (Exam Topic 1)
Connections to the Check Point R81 Web API use what protocol?

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

Answer: A

NEW QUESTION 67
- (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 69
- (Exam Topic 1)
Which command lists all tables in Gaia?

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

Answer: C

NEW QUESTION 71
- (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 76
- (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 79
- (Exam Topic 1)
Which two of these Check Point Protocols are used by SmartEvent Processes?

A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG

Answer: D

NEW QUESTION 81
- (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 82
- (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 84
- (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 85
- (Exam Topic 1)
CPM process stores objects, policies, users, administrators, licenses and management data in a database. The database is:

A. MySQL
B. Postgres SQL
C. MarisDB
D. SOLR

Answer: B

NEW QUESTION 87
- (Exam Topic 2)
Both ClusterXL and VRRP are fully supported by Gaia R81.10 and available to all Check Point appliances. Which the following command is NOT related to redundancy and functions?

A. cphaprob stat
B. cphaprob –a if
C. cphaprob –l list
D. cphaprob all show stat

Answer: D

NEW QUESTION 89
- (Exam Topic 2)
John is using Management HA. Which Smartcenter should be connected to for making changes?

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

Answer: B

NEW QUESTION 92
- (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 97
- (Exam Topic 2)
Which GUI client is supported in R81?

A. SmartProvisioning
B. SmartView Tracker

C. SmartView Monitor
D. SmartLog

Answer: C

NEW QUESTION 101

- (Exam Topic 2)
Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

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

Answer: D

Explanation:
Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that requite direct GUI access, such as SmartEvent,
It provides the following:
– GUI Client communication
– Database manipulation
– Policy Compilation
– Management HA sync

NEW QUESTION 105

- (Exam Topic 2)
Which of the following describes how Threat Extraction functions?

A. Detect threats and provides a detailed report of discovered threats.
B. Proactively detects threats.
C. Delivers file with original content.
D. Delivers PDF versions of original files with active content removed.

Answer: B

NEW QUESTION 108

- (Exam Topic 2)
You find one of your cluster gateways showing "Down" when you run the "cphaprob stat" command. You then run the "clusterXL_admin up" on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

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

Answer: D

NEW QUESTION 110

- (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 113

- (Exam Topic 2)
What is the protocol and port used for Health Check and State Synchronization in ClusterXL?

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

Answer: C

NEW QUESTION 117

- (Exam Topic 2)
For Management High Availability, which of the following is NOT a valid synchronization status?

A. Collision
B. Down
C. Lagging

D. Never been synchronized

Answer: B

NEW QUESTION 119
- (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 122
- (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 127
- (Exam Topic 2)
How often does Threat Emulation download packages by default?

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

Answer: D

NEW QUESTION 132
- (Exam Topic 2)
What is the name of the secure application for Mail/Calendar for mobile devices?

A. Capsule Workspace
B. Capsule Mail
C. Capsule VPN
D. Secure Workspace

Answer: A

NEW QUESTION 133
- (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 135
- (Exam Topic 2)
You have existing dbedit scripts from R77. Can you use them with R81.10?

A. dbedit is not supported in R81.10
B. dbedit is fully supported in R81.10
C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
D. dbedit scripts are being replaced by mgmt_cli in R81.10

Answer: D

NEW QUESTION 139
- (Exam Topic 2)
What is a best practice before starting to troubleshoot using the "fw monitor" tool?

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

Answer: D

NEW QUESTION 142
- (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 145
- (Exam Topic 2)
When simulating a problem on ClusterXL cluster with cphaprob –d STOP -s problem -t 0 register, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

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

Answer: A

Explanation:
esting a failover in a controlled manner using following command;
cphaprob -d STOP -s problem -t 0 register
This will register a problem state on the cluster member this was entered on; If you then run;
cphaprob list
this will show an entry named STOP.
to remove this problematic register run following;
cphaprob -d STOP unregister References:

NEW QUESTION 150
- (Exam Topic 2)
Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 155
- (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 157
- (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 160
- (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 164
- (Exam Topic 2)
What is mandatory for ClusterXL to work properly?

A. The number of cores must be the same on every participating cluster node
B. The Magic MAC number must be unique per cluster node
C. The Sync interface must not have an IP address configured
D. If you have "Non-monitored Private" interfaces, the number of those interfaces must be the same on all cluster members

Answer: B

NEW QUESTION 168
- (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 173
- (Exam Topic 2)
What is the purpose of Priority Delta in VRRP?

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

Answer: C

Explanation:
Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP. If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will beging to send out its own HELLO packet. Once the master sees this packet with a priority greater than its own, then it releases the VIP. References:

NEW QUESTION 176
- (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 179
- (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 181
- (Exam Topic 2)
Which directory below contains log files?

A. /opt/CPSmartlog-R81/log

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

Answer: C

NEW QUESTION 182
- (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 185
- (Exam Topic 2)
What is the most recommended way to install patches and hotfixes?

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

Answer: A

NEW QUESTION 188
- (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 192
- (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 195
- (Exam Topic 2)
What are the steps to configure the HTTPS Inspection Policy?

A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: A

NEW QUESTION 200
- (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 201
- (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 205
- (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 210
- (Exam Topic 2)
Which of the following links will take you to the SmartView web application?

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

Answer: B

NEW QUESTION 214
- (Exam Topic 2)
When installing a dedicated R81 SmartEvent server. What is the recommended size of the root partition?

A. Any size
B. Less than 20GB
C. More than 10GB and less than 20GB
D. At least 20GB

Answer: D

NEW QUESTION 217
- (Exam Topic 2)
Which web services protocol is used to communicate to the Check Point R81 Identity Awareness Web API?

A. SOAP
B. REST
C. XLANG
D. XML-RPC

Answer: B

Explanation:
The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

NEW QUESTION 221
- (Exam Topic 2)
SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

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

Answer: A

NEW QUESTION 225
- (Exam Topic 2)
Automation and Orchestration differ in that:

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

Answer: A

NEW QUESTION 227
- (Exam Topic 2)
Which command gives us a perspective of the number of kernel tables?

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

Answer: B

NEW QUESTION 229
- (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 234
- (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 238
- (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 240
- (Exam Topic 3)
Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 244
- (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 247

- (Exam Topic 3)
How many policy layers do Access Control policy support?

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

Answer: A

Explanation:
Two policy layers:
- Network Policy Layer
- Application Control Policy Layer

NEW QUESTION 252
- (Exam Topic 3)
What is true of the API server on R81.10?

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

Answer: D

NEW QUESTION 255
- (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 statement is most correct regarding about "CoreXL Dynamic Dispatcher"?

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

Answer: B

NEW QUESTION 261
- (Exam Topic 3)
GAiA Software update packages can be imported and installed offline in situation where:

A. Security Gateway with GAiA does NOT have SFTP access to Internet
B. Security Gateway with GAiA does NOT have access to Internet.
C. Security Gateway with GAiA does NOT have SSH access to Internet.
D. The desired CPUSE package is ONLY available in the Check Point CLOUD.

Answer: B

NEW QUESTION 265
- (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 266
- (Exam Topic 3)
Fill in the blank: The "fw monitor" tool can be best used to troubleshoot _____.

A. AV issues
B. VPN errors

C. Network traffic issues
D. Authentication issues

Answer: C

Explanation:
 https://supportcenter.checkpoint.com/supportcenter/portal? eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

NEW QUESTION 267
- (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 269
- (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 270
- (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 275
- (Exam Topic 3)
One of major features in R81 SmartConsole is concurrent administration.
Which of the following is NOT possible considering that AdminA, AdminB and AdminC are editing the same Security Policy?

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

Answer: C

NEW QUESTION 277
- (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 282
- (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 283
- (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 288
- (Exam Topic 3)
What CLI command compiles and installs a Security Policy on the target's Security Gateways?

A. fwm compile
B. fwm load
C. fwm fetch
D. fwm install

Answer: B

NEW QUESTION 293
- (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 297
- (Exam Topic 3)
Which blades and or features are not supported in R81?

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

Answer: A

NEW QUESTION 301
- (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 302
- (Exam Topic 3)
After trust has been established between the Check Point components, what is TRUE about name and IP-address changes?

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

Answer: A

NEW QUESTION 303
- (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 305
- (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 310
- (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 314
- (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 319
- (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 323
- (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 324
- (Exam Topic 3)
Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment.
Which details she need to fill in System Restore window before she can click OK button and test the backup?

A. Server, SCP, Username, Password, Path, Comment, Member

B. Server, TFTP, Username, Password, Path, Comment, All Members
C. Server, Protocol, Username, Password, Path, Comment, All Members
D. Server, Protocol, username Password, Path, Comment, Member

Answer: C

NEW QUESTION 329
- (Exam Topic 3)
The system administrator of a company is trying to find out why acceleration is not working for the traffic. The traffic is allowed according to the rule base and checked for viruses. But it is not accelerated.
What is the most likely reason that the traffic is not accelerated?

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

Answer: B

NEW QUESTION 331
- (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 332
- (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 334
- (Exam Topic 3)
Ken wants to obtain a configuration lock from other administrator on R81 Security Management Server. He can do this via WebUI or via CLI.
Which command should he use in CLI? (Choose the correct answer.)

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

Answer: D

NEW QUESTION 339
- (Exam Topic 3)
Which path below is available only when CoreXL is enabled?

A. Slow path
B. Firewall path
C. Medium path
D. Accelerated path

Answer: C

NEW QUESTION 341
- (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 343
- (Exam Topic 3)
How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 348
- (Exam Topic 3)
In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Stateful Mode configuration, chain modules marked with _____ will not apply.

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

Answer: D

NEW QUESTION 352
- (Exam Topic 3)
For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

A. 20 minutes
B. 15 minutes
C. Admin account cannot be unlocked automatically
D. 30 minutes at least

Answer: D

NEW QUESTION 355
- (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 358
- (Exam Topic 3)
Which of the following is NOT an alert option?

A. SNMP
B. High alert
C. Mail
D. User defined alert

Answer: B

NEW QUESTION 361
- (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 362
- (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 365
- (Exam Topic 4)
Firewall polices must be configured to accept VRRP packets on the GAiA platform if it Firewall software. The Multicast destination assigned by the internet Assigned Number Authority (IANA) for VRRP is:

A. 224.0.0.18
B. 224 00 5
C. 224.0.0.102
D. 224.0.0.22

Answer: A

NEW QUESTION 367
- (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 368
- (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 370
- (Exam Topic 4)
What is the default size of NAT table fwx_alloc?

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

Answer: C

NEW QUESTION 371
- (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 374
- (Exam Topic 4)
Which command lists firewall chain?

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

Answer: A

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

NEW QUESTION 377
- (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?
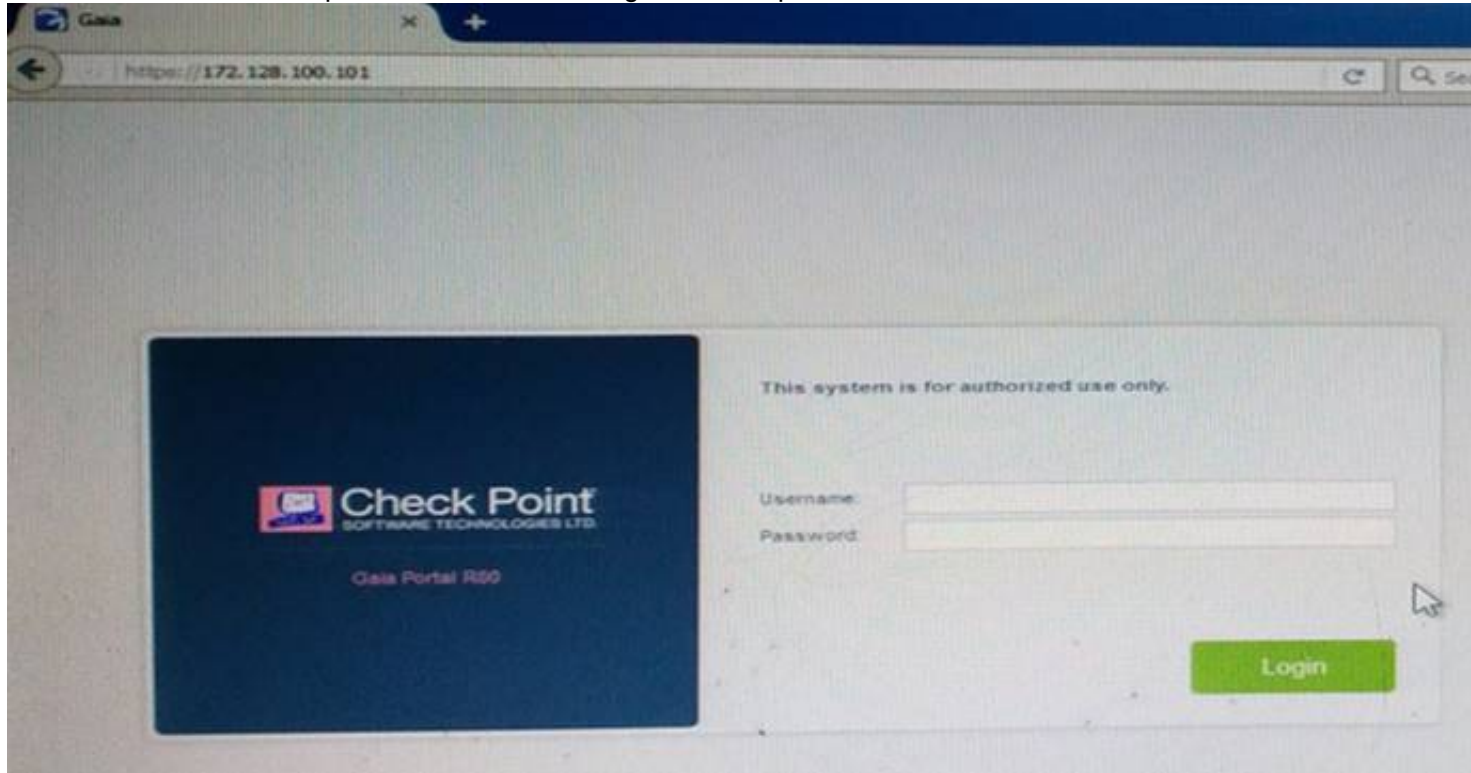
A. set web ssl-port <new port number>
B. set Gaia-portal port <new port number>
C. set Gaia-portal https-port <new port number>
D. set web https-port <new port number>

Answer: A

NEW QUESTION 379
- (Exam Topic 4)
Installations and upgrades with CPUSE require that the CPUSE agent is up-to-date. Usually the latest build is downloaded automatically. How can you verify the CPUSE agent build?

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

Answer: A

NEW QUESTION 380
- (Exam Topic 4)
Which components allow you to reset a VPN tunnel?

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

Answer: D

NEW QUESTION 384
- (Exam Topic 4)
There are multiple types of licenses for the various VPN components and types. License type related to management and functioning of Remote Access VPNs are - which of the following license requirement statement is NOT true:

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

Answer: C

NEW QUESTION 388
- (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 389
- (Exam Topic 4)
Fill in the blanks: A _____ license requires an administrator to designate a gateway for attachment whereas a _____ license is automatically attached to a Security Gateway.

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

Answer: D

NEW QUESTION 394
- (Exam Topic 4)
What is the SOLR database for?

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

Answer: A

NEW QUESTION 398
- (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 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 406
- (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 410
- (Exam Topic 4)
What are the modes of SandBlast Threat Emulation deployment?

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

Answer: D

NEW QUESTION 412
- (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 415
- (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 416
- (Exam Topic 4)
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

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

Answer: B

NEW QUESTION 418
- (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 421
- (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 422
- (Exam Topic 4)
After having saved the Clish Configuration with the "save configuration config.txt" command, where can you find the config.txt file?

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

Answer: A

NEW QUESTION 425
- (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 429
- (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 430
- (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 432
- (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 433
- (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 434
- (Exam Topic 4)
GAIA greatly increases operational efficiency by offering an advanced and intuitive software update agent, commonly referred to as the:

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

Answer: A

NEW QUESTION 435
- (Exam Topic 4)
What are the correct sleps upgrading a HA cluster (MI is active. M2 is passive) using Multi-Version Cluster(MVC) Upgrade?

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

H. 1) Upgrade the passive node M2 to R81.102) Enable the MVC mechanism on the upgraded R81.10 Cluster Member M2 ttcphaconf mvc on3) In SmartConsole, change the version of the cluster object 4} Install the Access Control Policy5) After examine the cluster states upgrade node M1 to R81.106) On each Cluster Member, disable the MVC mechanism and Install the Access Control Policy upgrade the passive node M2 to R81.10

Answer: D

NEW QUESTION 440
- (Exam Topic 4)
What is a possible command to delete all of the SSH connections of a gateway?

A. fw sam -I 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 441
- (Exam Topic 4)
Within the Check Point Firewall Kernel resides Chain Modules, which are individually responsible for the inspection of a specific blade or feature that has been enabled in the configuration of the gateway. For Wire mode configuration, chain modules marked with _____ will not apply.

A. ffffffff
B. 00000001
C. 00000002
D. 00000003

Answer: B

NEW QUESTION 442
- (Exam Topic 4)
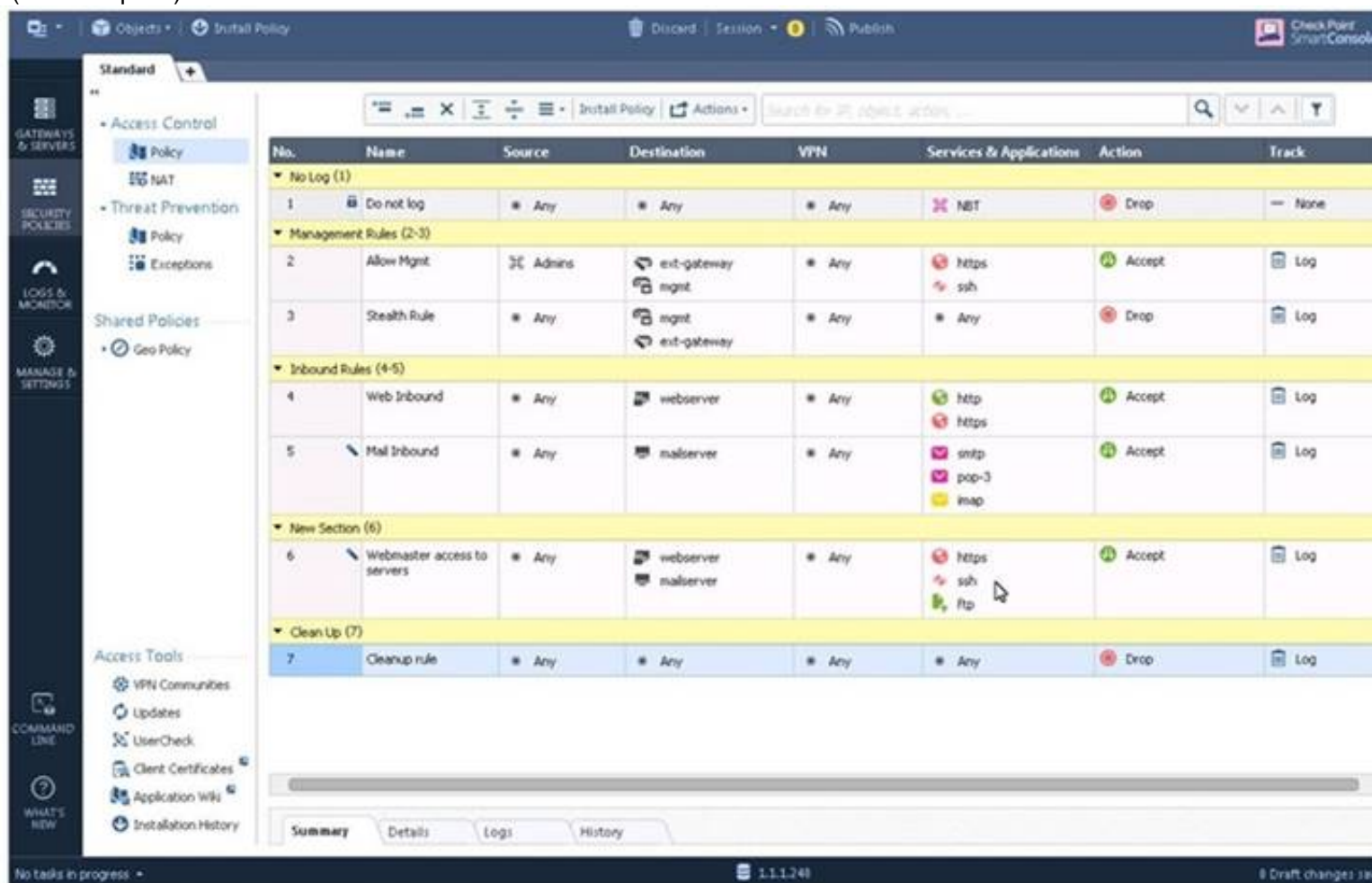Due to high CPU workload on the Security Gateway, the security administrator decided to purchase a new CPU to replace the existing single core CPU. After installation, is the administrator required to perform any additional tasks?

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 445
- (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 448
- (Exam Topic 4)
Fill in the blank: An identity server uses a _____ for user authentication.

A. Shared secret
B. Certificate
C. One-time password
D. Token

Answer: A

NEW QUESTION 452
- (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 453
- (Exam Topic 4)
What is the valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration?

A. 1-254
B. 1-255
C. 0-254
D. 0 – 255

Answer: B

NEW QUESTION 456
- (Exam Topic 4)
How many versions, besides the destination version, are supported in a Multi-Version Cluster Upgrade?

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

Answer: B

NEW QUESTION 459
- (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. Run cprestart from clish
B. After upgrading the hardware, increase the number of kernel instances using cpconfig
C. Administrator does not need to perform any tas
D. Check Point will make use of the newly installed CPU and Cores
E. Hyperthreading must be enabled in the bios to use CoreXL

Answer: B

NEW QUESTION 461
- (Exam Topic 4)

What can we infer about the recent changes made to the Rule Base?

A. Rule 7 was created by the 'admin' administrator in the current session
B. 8 changes have been made by administrators since the last policy installation
C. The rules 1, 5 and 6 cannot be edited by the 'admin' administrator
D. Rule 1 and object webserver are locked by another administrator

Answer: D

NEW QUESTION 464
- (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 465
- (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 467
- (Exam Topic 4)
Which of the following is NOT supported by CPUSE?

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

Answer: D

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

NEW QUESTION 469
- (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 470
- (Exam Topic 4)
What is the correct order of the default "fw monitor" inspection points?

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

Answer: C

NEW QUESTION 471
- (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 475
- (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 476
- (Exam Topic 4)
Bob is asked by Alice to disable the SecureXL mechanism temporary tor further diagnostic by their Check Point partner. Which of the following Check Point Command is true:

A. fwaccel suspend
B. fwaccel standby
C. fwaccel off
D. fwaccel templates

Answer: C

NEW QUESTION 479
- (Exam Topic 4)
Which component is NOT required to communicate with the Web Services API?

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

Answer: A

NEW QUESTION 483
- (Exam Topic 4)
Which member of a high-availability cluster should be upgraded first in a Zero downtime upgrade?

A. The Standby Member
B. The Active Member
C. The Primary Member
D. The Secondary Member

Answer: A

NEW QUESTION 484
- (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 489
- (Exam Topic 4)
What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

A. Use Multi-Domain Management Server.
B. Choose different setting for log storage and SmartEvent db
C. Install Management and SmartEvent on different machines.
D. it is not possible.

Answer: C

NEW QUESTION 490
- (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 495
- (Exam Topic 4)
Packet acceleration (SecureXL) identifies connections by several attributes- Which of the attributes is NOT used for identifying connection?

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

Answer: C

Explanation:
https //sc1.checkpoint.com/documents/R77/CP R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 499
- (Exam Topic 4)
Bob has finished io setup provisioning a secondary security management server. Now he wants to check if the provisioning has been correct. Which of the following Check Point command can be used to check if the security management server has been installed as a primary or a secondary security management server?

A. cpprod_util MgmtlsPrimary
B. cpprod_util FwlsSecondary
C. cpprod_util MgmtlsSecondary
D. cpprod_util FwlsPrimary

Answer: A

NEW QUESTION 504
- (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 508
- (Exam Topic 4)
By default, the R81 web API uses which content-type in its response?

A. Java Script
B. XML
C. Text
D. JSON

Answer: D

NEW QUESTION 511
- (Exam Topic 4)
When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

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

Answer: D

NEW QUESTION 515
- (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_Adress>
B. http://<Device IP_Address>:443
C. https://<Device_IP_Address>:10000
D. https://<Device_IP_Address>:4434

Answer: A

NEW QUESTION 518
- (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 523
- (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 526
- (Exam Topic 4)
In Advanced Permanent Tunnel Configuration, to set the amount of time the tunnel test runs without a response before the peer host is declared 'down', you would set the ?

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

Answer: D

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

NEW QUESTION 527
- (Exam Topic 4)
SandBlast agent extends 0 day prevention to what part of the network?

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

Answer: A

NEW QUESTION 532
- (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 536
- (Exam Topic 4)
What are the available options for downloading Check Point hotfixes in Gala WebUI (CPUSE)?

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

Answer: A

Explanation:

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

NEW QUESTION 540
- (Exam Topic 4)
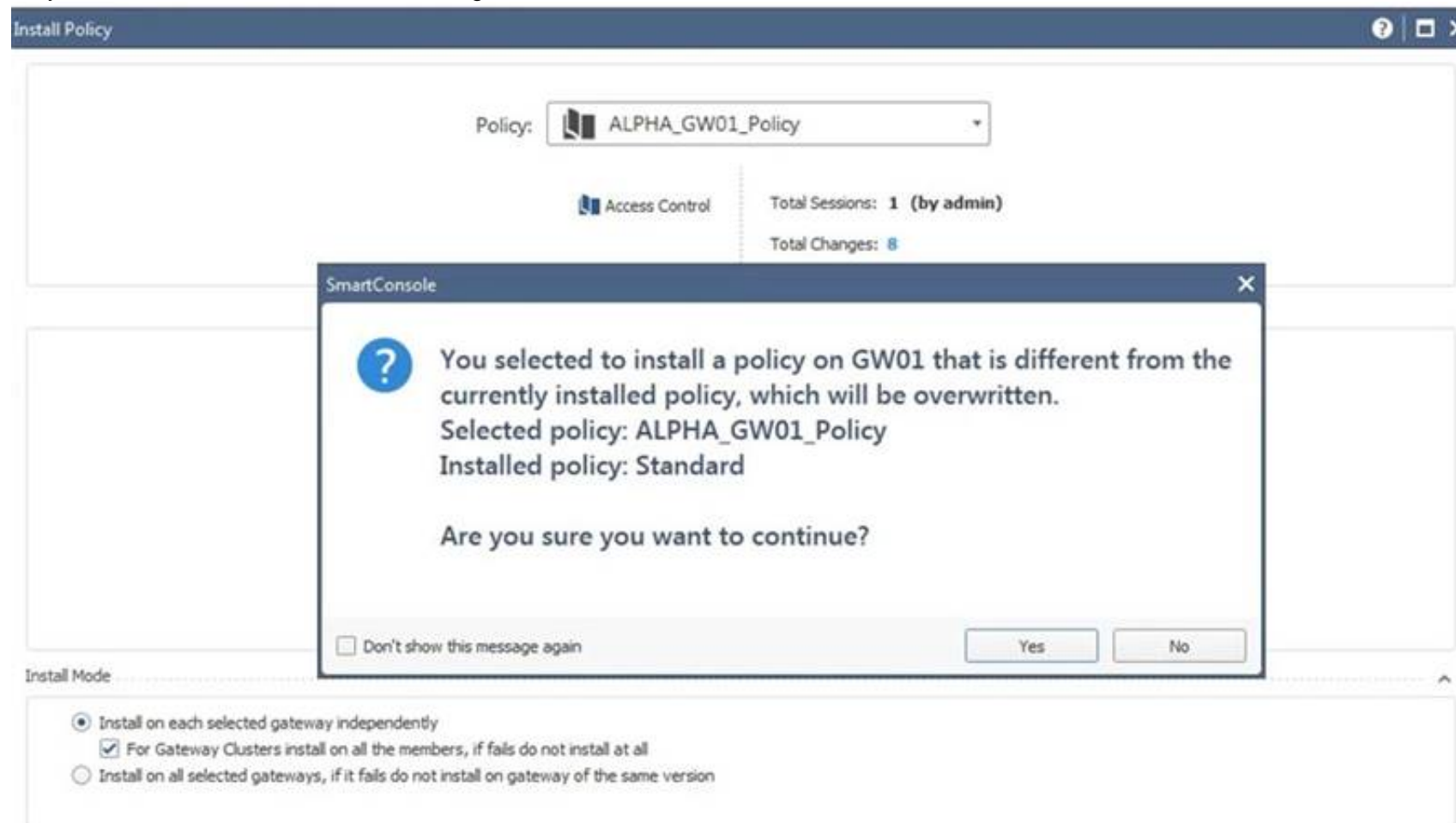What two ordered layers make up the Access Control Policy Layer?

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 545
- (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 550
- (Exam Topic 4)
What component of Management is used tor 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 553
- (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 558
- (Exam Topic 4)
If there are two administration logged in at the same time to the SmartConsole, and there are objects locked for editing, what must be done to make them available or other administrators? (Choose the BEST answer.)

A. Publish or discard the session.
B. Revert the session.
C. Save and install the Policy.
D. Delete older versions of database.

Answer: A

NEW QUESTION 559
- (Exam Topic 4)
How can you switch the active log file?

A. Run fw logswitch on the gateway
B. Run fwm logswitch on the Management Server
C. Run fwm logswitch on the gateway
D. Run fw logswitch on the Management Server

Answer: D

NEW QUESTION 563
- (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:
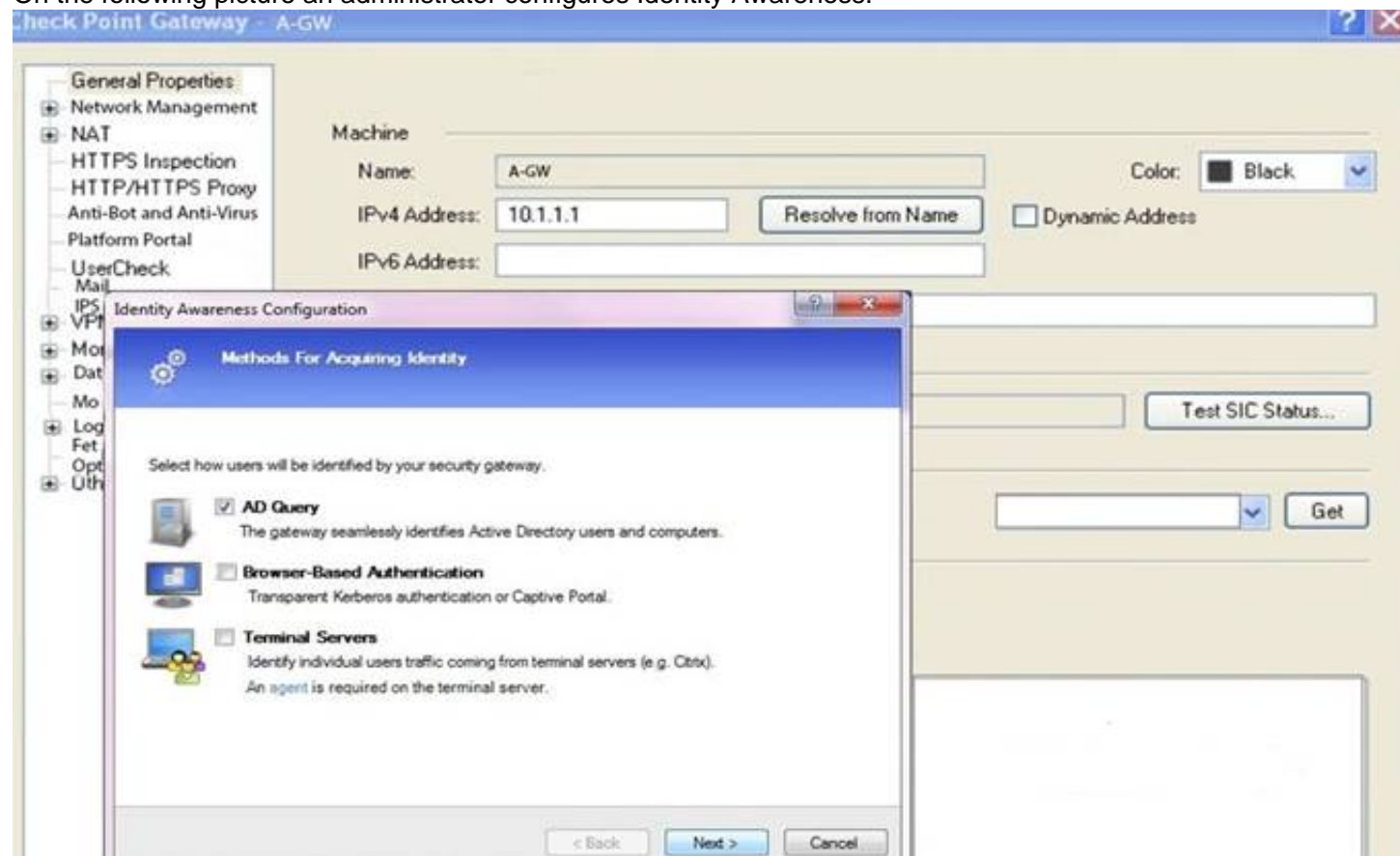
A. ReverseCLIProxy
B. ReverseProxyCLI
C. ReverseProxy
D. ProxyReverseCLI

Answer: C

NEW QUESTION 568
- (Exam Topic 4)
On the following picture an administrator configures Identity Awareness:

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

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

Answer: B

NEW QUESTION 572
- (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 576
- (Exam Topic 4)
Which of the following is NOT an attribute of packet acceleration?

A. Source address
B. Protocol
C. Destination port
D. VLAN Tag

Answer: D

NEW QUESTION 581
- (Exam Topic 4)
The log server sends what to the Correlation Unit?

A. Authentication requests
B. CPMI dbsync
C. Logs
D. Event Policy

Answer: C

NEW QUESTION 585
- (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 587
- (Exam Topic 4)
To optimize Rule Base efficiency, the most hit rules should be where?

A. Removed from the Rule Base.
B. Towards the middle of the Rule Base.
C. Towards the top of the Rule Base.
D. Towards the bottom of the Rule Base.

Answer: C

NEW QUESTION 590
- (Exam Topic 4)
Secure Configuration Verification (SCV), makes sure that remote access client computers are configured in accordance with the enterprise Security Policy. Bob was asked by Alice to implement a specific SCV configuration but therefore Bob needs to edit and configure a specific Check Point file. Which location file and directory is true?

A. $FWDIR/conf/client.scv
B. $CPDIR/conf/local.scv
C. $CPDIR/conf/client.svc
D. $FWDIR/conf/local.scv

Answer: D

Explanation:
https://sc1.checkpoint.com/documents/R81.10/WebAdminGuides/EN/CP_R81.10_RemoteAccessVPN_AdminG

NEW QUESTION 593
- (Exam Topic 4)
SmartEvent uses it's event policy to identify events. How can this be customized?

A. By modifying the firewall rulebase
B. By creating event candidates
C. By matching logs against exclusions
D. By matching logs against event rules

Answer: D

NEW QUESTION 598
- (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 603
- (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 605
- (Exam Topic 4)
Fill in the blank: The IPS policy for pre-R81 gateways is installed during the _____ .

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

Answer: C

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

NEW QUESTION 610
......

Relate Links

100% Pass Your 156-315.81 Exam with Exambible Prep Materials

https://www.exambible.com/156-315.81-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/