CheckPoint

Exam Questions 156-315.81

Check Point Certified Security Expert R81

About Exambible

Your Partner of IT Exam

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 these statements describes the Check Point ThreatCloud?

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

Answer: D

NEW QUESTION 3
- (Exam Topic 1)
fwssd is a child process of which of the following Check Point daemons?

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

Answer: A

NEW QUESTION 4
- (Exam Topic 1)
Check Pont Central Deployment Tool (CDT) communicates with the Security Gateway / Cluster Members over Check Point SIC _____.

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

Answer: D

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

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

Answer: B

NEW QUESTION 7
- (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 8
- (Exam Topic 1)
You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?

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

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
Which command can you use to enable or disable multi-queue per interface?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 1)
You want to gather and analyze threats to your mobile device. It has to be a lightweight app. Which application would you use?

A. SmartEvent Client Info
B. SecuRemote
C. Check Point Protect
D. Check Point Capsule Cloud

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?

A. Secure Internal Communication (SIC)
B. Restart Daemons if they fail
C. Transfers messages between Firewall processes
D. Pulls application monitoring status

Answer: D

NEW QUESTION 13
- (Exam Topic 1)
Which TCP-port does CPM process listen to?

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

Answer: D

NEW QUESTION 18
- (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 19
- (Exam Topic 1)
The Security Gateway is installed on GAIA R81. The default port for the Web User Interface is _____.

A. TCP 18211
B. TCP 257
C. TCP 4433
D. TCP 443

Answer: D

NEW QUESTION 20
- (Exam Topic 1)
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 21
- (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 26
- (Exam Topic 1)
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _____.

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

Answer: A

NEW QUESTION 31
- (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 33
- (Exam Topic 1)
During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

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

Answer: D

NEW QUESTION 34
- (Exam Topic 1)
Your manager asked you to check the status of SecureXL, and its enabled templates and features. What command will you use to provide such information to

manager?

A. fw accel stat
B. fwaccel stat
C. fw acces stats
D. fwaccel stats

Answer: B

NEW QUESTION 35
- (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 40
- (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 45
- (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 48
- (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 50
- (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 51
- (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 54
- (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 56
- (Exam Topic 1)
Which of the following type of authentication on Mobile Access can NOT be used as the first authentication method?

A. Dynamic ID
B. RADIUS
C. Username and Password
D. Certificate

Answer: A

NEW QUESTION 59
- (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 60
- (Exam Topic 1)
In R81 spoofing is defined as a method of:

A. Disguising an illegal IP address behind an authorized IP address through Port Address Translation.
B. Hiding your firewall from unauthorized users.
C. Detecting people using false or wrong authentication logins
D. Making packets appear as if they come from an authorized IP address.

Answer: D

Explanation:
IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

NEW QUESTION 61
- (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 65
- (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 70
- (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 74
- (Exam Topic 2)
What is the main difference between Threat Extraction and Threat Emulation?

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

Answer: B

NEW QUESTION 79
- (Exam Topic 2)
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

A. This statement is true because SecureXL does improve all traffic.
B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
C. This statement is true because SecureXL does improve this traffic.
D. This statement is false because encrypted traffic cannot be inspected.

Answer: C

Explanation:
SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.

NEW QUESTION 84
- (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 86
- (Exam Topic 2)
Which of the following will NOT affect acceleration?

A. Connections destined to or originated from the Security gateway
B. A 5-tuple match
C. Multicast packets
D. Connections that have a Handler (ICMP, FTP, H.323, etc.)

Answer: B

NEW QUESTION 88
- (Exam Topic 2)
How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

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

Answer: C

NEW QUESTION 89
- (Exam Topic 2)
What information is NOT collected from a Security Gateway in a Cpinfo?

A. Firewall logs
B. Configuration and database files
C. System message logs
D. OS and network statistics

Answer: A

NEW QUESTION 91
- (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 96
- (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 97
- (Exam Topic 2)
Please choose correct command to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

A. host name myHost12 ip-address 10.50.23.90
B. mgmt: add host name ip-address 10.50.23.90
C. add host name emailserver1 ip-address 10.50.23.90
D. mgmt: add host name emailserver1 ip-address 10.50.23.90

Answer: D

NEW QUESTION 102
- (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 107
- (Exam Topic 2)
The Correlation Unit performs all but the following actions:

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

Answer: C

NEW QUESTION 112
- (Exam Topic 2)
Which command shows detailed information about VPN tunnels?

A. cat $FWDIR/conf/vpn.conf
B. vpn tu tlist
C. vpn tu
D. cpview

Answer: B

NEW QUESTION 117
- (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 122
- (Exam Topic 2)
When an encrypted packet is decrypted, where does this happen?

A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported

Answer: A

NEW QUESTION 124
- (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 127
- (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 131
- (Exam Topic 2)
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enabled which path is handling the traffic?

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

Answer: A

NEW QUESTION 136
- (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 137
- (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 142

- (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 147
- (Exam Topic 2)
You want to store the GAIA configuration in a file for later reference. What command should you use?

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

Answer: D

NEW QUESTION 151
- (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 155
- (Exam Topic 2)
What component of R81 Management is used for indexing?

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

Answer: D

NEW QUESTION 160
- (Exam Topic 2)
SandBlast appliances can be deployed in the following modes:

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

Answer: C

NEW QUESTION 163
- (Exam Topic 3)
Fill in the blank: Identity Awareness AD-Query is using the Microsoft _____ API to learn users from AD.

A. WMI
B. Eventvwr
C. XML
D. Services.msc

Answer: A

NEW QUESTION 164
- (Exam Topic 3)
Which is NOT a SmartEvent component?

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

Answer: C

NEW QUESTION 166
- (Exam Topic 3)
What statement best describes the Proxy ARP feature for Manual NAT in R81.10?

A. Automatic proxy ARP configuration can be enabled
B. Translate Destination on Client Side should be configured
C. fw ctl proxy should be configured
D. local.arp file must always be configured

Answer: D

NEW QUESTION 170
- (Exam Topic 3)
What is the Implicit Clean-up Rule?

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

Answer: C

NEW QUESTION 174
- (Exam Topic 3)
Tom has connected to the R81 Management Server remotely using SmartConsole and is in the process of making some Rule Base changes, when he suddenly loses connectivity. Connectivity is restored shortly afterward.
What will happen to the changes already made?

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

Answer: A

NEW QUESTION 178
- (Exam Topic 3)
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/R81.10. Company's Developer Team is having random access issue to newly deployed Application Server in DMZ's Application Server Farm Tier and blames DMZ Security Gateway as root cause. The ticket has been created and issue is at Pamela's desk for an investigation. Pamela decides to use Check Point's Packet Analyzer Tool-fw monitor to iron out the issue during approved Maintenance window.
What do you recommend as the best suggestion for Pamela to make sure she successfully captures entire traffic in context of Firewall and problematic traffic?

A. Pamela should check SecureXL status on DMZ Security gateway and if it's turned O
B. She should turn OFF SecureXL before using fw monitor to avoid misleading traffic captures.
C. Pamela should check SecureXL status on DMZ Security Gateway and if it's turned OF
D. She should turn ON SecureXL before using fw monitor to avoid misleading traffic captures.
E. Pamela should use tcpdump over fw monitor tool as tcpdump works at OS-level and captures entire traffic.
F. Pamela should use snoop over fw monitor tool as snoop works at NIC driver level and captures entire traffic.

Answer: A

NEW QUESTION 179
- (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 181
- (Exam Topic 3)
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 184
- (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 187
- (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 190
- (Exam Topic 3)
What is UserCheck?

A. Messaging tool used to verify a user’s credentials.
B. Communication tool used to inform a user about a website or application they are trying to access.
C. Administrator tool used to monitor users on their network.
D. Communication tool used to notify an administrator when a new user is created.

Answer: B

NEW QUESTION 194
- (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 196
- (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 201
- (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 204
- (Exam Topic 3)
What is the order of NAT priorities?

A. Static NAT, IP pool NAT, hide NAT
B. IP pool NAT, static NAT, hide NAT
C. Static NAT, automatic NAT, hide NAT
D. Static NAT, hide NAT, IP pool NAT

Answer: A

NEW QUESTION 209
- (Exam Topic 3)
What is the command to show SecureXL status?

A. fwaccel status
B. fwaccel stats -m
C. fwaccel -s
D. fwaccel stat

Answer: D

Explanation:
To check overall SecureXL status: [Expert@HostName]# fwaccel stat References:

NEW QUESTION 210
- (Exam Topic 3)
You want to verify if your management server is ready to upgrade to R81.10. What tool could you use in this process?

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

Answer: C

NEW QUESTION 211
- (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 212
- (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 216
- (Exam Topic 3)
What are the methods of SandBlast Threat Emulation deployment?

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

Answer: A

NEW QUESTION 217
- (Exam Topic 3)
You notice that your firewall is under a DDoS attack and would like to enable the Penalty Box feature, which command you use?

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

Answer: A

NEW QUESTION 219
- (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 220
- (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 221
- (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 222
- (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 223
- (Exam Topic 4)
You work as a security administrator for a large company. CSO of your company has attended a security conference where he has learnt how hackers constantly modify their strategies and techniques to evade detection and reach corporate resources. He wants to make sure that his company has the tight protections in place. Check Point has been selected for the security vendor.
Which Check Point product protects BEST against malware and zero-day attacks while ensuring quick delivery of safe content to your users?

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

Answer: D

NEW QUESTION 224
- (Exam Topic 4)
Matt wants to upgrade his old Security Management server to R81.x using the Advanced Upgrade with Database Migration. What is one of the requirements for a successful upgrade?

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

Answer: B

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

NEW QUESTION 226

- (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 231
- (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 235
- (Exam Topic 4)
The “Hit count” feature allows tracking the number of connections that each rule matches. Will the Hit count feature work independently from logging and Track the hits if the Track option is set to “None”?

A. No, it will work independentl
B. Hit Count will be shown only for rules Track option set as Log or alert.
C. Yes it will work independently as long as “analyze all rules” tick box is enabled on the Security Gateway.
D. No, it will not work independently because hit count requires all rules to be logged.
E. Yes it will work independently because when you enable Hit Count, the SMS collects the data from supported Security Gateways.

Answer: D

NEW QUESTION 238
- (Exam Topic 4)
Which of the following is an identity acquisition method that allows a Security Gateway to identify Active Directory users and computers?

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

Answer: B

Explanation:
Reference : https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

NEW QUESTION 242
- (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 244
- (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 249
- (Exam Topic 4)
You need to change the MAC-address on eth2 interface of the gateway. What command and what mode will you use to achieve this goal?

A. set interface eth2 mac-addr 11:11:11:11:11:11; CLISH

B. ifconfig eth1 hw 11:11:11:11:11:11; expert
C. set interface eth2 hw-addr 11:11:11:11:11:11; CLISH
D. ethtool -i eth2 mac 11:11:11:11:11:11; expert

Answer: A

NEW QUESTION 253
- (Exam Topic 4)
Fill in the blank: Permanent VPN tunnels can be set on all tunnels in the community, on all tunnels for specific gateways, or _____.

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

Answer: C

NEW QUESTION 258
- (Exam Topic 4)
According to out of the box SmartEvent policy, which blade will automatically be correlated into events?

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

Answer: C

NEW QUESTION 262
- (Exam Topic 4)
Fill in the blanks: In the Network policy layer, the default action for the Implied last rule is _____ all traffic. However, in the Application Control policy layer, the default action is _____ all traffic.

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

Answer: D

NEW QUESTION 264
- (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-R7730	Any	https ssh	Accept	Log	Policy Targets
3	Stealth	Any	GW-R7730	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 267
- (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 271
- (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 276
- (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 277
- (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 278
- (Exam Topic 4)
What Is the difference between Updatable Objects and Dynamic Objects

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

Answer: B

NEW QUESTION 281
- (Exam Topic 4)
What is false regarding a Management HA environment?

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

Answer: B

NEW QUESTION 282
- (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 285
- (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 287
- (Exam Topic 4)
Which command shows only the table names of all kernel tables?

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

Answer: A

NEW QUESTION 290
- (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 292
- (Exam Topic 4)
Main Mode in IKEv1 uses how many packages for negotiation?

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

Answer: C

NEW QUESTION 293
- (Exam Topic 4)
Is it possible to establish a VPN before the user login to the Endpoint Client?

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

Answer: D

NEW QUESTION 298
- (Exam Topic 4)
Which of the following is a task of the CPD process?

A. Invoke and monitor critical processes and attempts to restart them if they fail
B. Transfers messages between Firewall processes
C. Log forwarding
D. Responsible for processing most traffic on a security gateway

Answer: B

Explanation:
https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12496.htm

NEW QUESTION 302
- (Exam Topic 4)
What API command below creates a new host object with the name "My Host" and IP address of "192 168 0 10"?

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

Answer: A

NEW QUESTION 305
- (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 309
- (Exam Topic 4)
What is the command to check the status of Check Point processes?

A. top
B. cptop
C. cphaprob list
D. cpwd_admin list

Answer: D

NEW QUESTION 314
- (Exam Topic 4)
When performing a minimal effort upgrade, what will happen to the network traffic?

A. All connections that were Initiated before the upgrade will be dropped, causing network downtime.
B. All connections that were initiated before the upgrade will be handled by the active gateway
C. All connections that were initiated before the upgrade will be handled normally
D. All connections that were initiated before the upgrade will be handled by the standby gateway

Answer: B

NEW QUESTION 318
- (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 323
- (Exam Topic 4)
What CLI utility runs connectivity tests from a Security Gateway to an AD domain controller?

A. test_connectivity_ad –d <domain>
B. test_ldap_connectivity –d <domain>
C. test_ad_connectivity –d <domain>
D. ad_connectivity_test –d <domain>

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R81.30/WebAdminGuides/EN/
CP_R81.30_CLI_ReferenceGuide/html_frameset.htm?topic=documents/R81.30/WebAdminGuides/EN/ CP_R81.30_CLI_ReferenceGuide/200877

NEW QUESTION 326
- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 331
- (Exam Topic 4)
You have pushed policy to GW-3 and now cannot pass traffic through the gateway. As a last resort, to restore traffic flow, what command would you run to remove the latest policy from GW-3?

A. fw unloadlocal
B. fw unloadpolicy
C. fwm unload local
D. fwm unload policy

Answer: A

NEW QUESTION 335
- (Exam Topic 4)
SmartConsole R81 x requires the following ports to be open for SmartEvent.

A. 19009, 19090 & 443
B. 19009, 19004 & 18190
C. 18190 & 443
D. 19009, 18190 & 443

Answer: D

NEW QUESTION 340
- (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 342
- (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 343
- (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 347
- (Exam Topic 4)
Which two Cluster Solutions are available under R81.10?

A. ClusterXL and NSRP
B. VRRPandHSRP
C. VRRP and IP Clustering
D. ClusterXL and VRitP

Answer: D

NEW QUESTION 349
- (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 351
- (Exam Topic 4)
What are the three SecureXL Templates available in R81.10?

A. PEP Template
B. QoS Template
C. VPN Templates
D. Accept Template
E. Drop Template
F. NAT Templates
G. Accept Template
H. Drop Template
I. Reject Templates
J. Accept Template
K. PDP Template
L. PEP Templates

Answer: B

NEW QUESTION 353
.....

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/