



Check-Point

Exam Questions 156-315.80

Check Point Certified Security Expert - R80

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

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 2

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 3

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. References:

NEW QUESTION 4

Using Threat Emulation technologies, what is the best way to block .exe and .bat file types?

- A. enable DLP and select.exe and .bat file type
- B. enable .exe & .bat protection in IPS Policy
- C. create FW rule for particular protocol
- D. tecli advanced attributes set prohibited_file_types exe.bat

Answer: A

NEW QUESTION 5

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

Explanation:

Note - References:

NEW QUESTION 6

When using the Mail Transfer Agent, where are the debug logs stored?

- A. \$FWDIR/bin/emaild.mt
- B. elg
- C. \$FWDIR/log/mtad elg
- D. /var/log/mail.mta elg
- E. \$CPDIR/log/emaild elg

Answer: A

NEW QUESTION 7

From SecureXL perspective, what are the tree paths of traffic flow:

- A. Initial Path; Medium Path; Accelerated Path

- B. Layer Path; Blade Path; Rule Path
- C. Firewall Path; Accept Path; Drop Path
- D. Firewall Path; Accelerated Path; Medium Path

Answer: D

NEW QUESTION 8

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 9

You want to verify if your management server is ready to upgrade to R80.10. 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 10

To fully enable Dynamic Dispatcher on a Security Gateway:

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

Answer: A

NEW QUESTION 10

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: A

Explanation:

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

NEW QUESTION 14

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 19

In R80 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 22

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 27

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 30

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 35

The Check Point history feature in R80 provides the following:

- A. View install changes and install specific version
B. View install changes
C. Policy Installation Date, view install changes and install specific version
D. Policy Installation Date only

Answer: C

NEW QUESTION 39

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 43

Which command can you use to verify the number of active concurrent connections?

- A. fw conn all
B. fw ctl pstat
C. show all connections
D. show connections

Answer: B

NEW QUESTION 46

In R80.10, 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 47

What is true of the API server on R80.10?

- 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 48

What scenario indicates that SecureXL is enabled?

- A. Dynamic objects are available in the Object Explorer
- B. SecureXL can be disabled in cpconfig
- C. fwaccel commands can be used in clish
- D. Only one packet in a stream is seen in a fw monitor packet capture

Answer: C

NEW QUESTION 50

Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:

- A. assign privileges to users.
- B. edit the home directory of the user.
- C. add users to your Gaia system.
- D. assign user rights to their home directory in the Security Management Server.

Answer: D

NEW QUESTION 51

What must you do first if “fwm sic_reset” could not be completed?

- A. Cpstop then find keyword “certificate” in objects_5_0.C and delete the section
- B. Reinitialize SIC on the security gateway then run “fw unloadlocal”
- C. Reset SIC from Smart Dashboard
- D. Change internal CA via cpconfig

Answer: D

NEW QUESTION 56

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 60

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

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

Answer: D

NEW QUESTION 64

The Security Gateway is installed on GAIA R80. 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 68

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

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

Answer: A

NEW QUESTION 73

Which file gives you a list of all security servers in use, including port number?

- A. \$FWDIR/conf/conf.conf
- B. \$FWDIR/conf/servers.conf
- C. \$FWDIR/conf/fwauthd.conf
- D. \$FWDIR/conf/serversd.conf

Answer: C

NEW QUESTION 77

To enable Dynamic Dispatch on Security Gateway without the Firewall Priority Queues, run the following command in Expert mode and reboot:

- A. fw ctl Dyn_Dispatch on
- B. fw ctl Dyn_Dispatch enable
- C. fw ctl multik set_mode 4
- D. fw ctl multik set_mode 1

Answer: C

NEW QUESTION 81

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 85

Which TCP-port does CPM process listen to?

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

Answer: D

NEW QUESTION 87

In SmartConsole, objects are used to represent physical and virtual network components and also some logical components. These objects are divided into several categories. Which of the following is NOT an objects category?

- A. Limit
- B. Resource
- C. Custom Application / Site
- D. Network Object

Answer: B

NEW QUESTION 91

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 95

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 96

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 99

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 103

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 108

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 112

R80.10 management server can manage gateways with which versions installed?

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

Answer: C

NEW QUESTION 114

What is the least amount of CPU cores required to enable CoreXL?

- A. 2
- B. 1
- C. 4
- D. 6

Answer: B

NEW QUESTION 119

What makes Anti-Bot unique compared to other Threat Prevention mechanisms, such as URL Filtering, Anti-Virus, IPS, and Threat Emulation?

- A. Anti-Bot is the only countermeasure against unknown malware
- B. Anti-Bot is the only protection mechanism which starts a counter-attack against known Command & Control Centers
- C. Anti-Bot is the only signature-based method of malware protection.
- D. Anti-Bot is a post-infection malware protection to prevent a host from establishing a connection to a Command & Control Center.

Answer: D

NEW QUESTION 120

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 125

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 129

What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 133

How many users can have read/write access in Gaia at one time?

- A. Infinite
- B. One
- C. Three
- D. Two

Answer: B

NEW QUESTION 138

Which command shows actual allowed connections in state table?

- A. fw tab -t StateTable
- B. fw tab -t connections
- C. fw tab -t connection
- D. fw tab connections

Answer: B

NEW QUESTION 139

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 142

SmartConsole R80 requires the following ports to be open for SmartEvent R80 management:

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

Answer: D

NEW QUESTION 143

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 145

When configuring SmartEvent Initial settings, you must specify a basic topology for SmartEvent to help it calculate traffic direction for events. What is this setting called and what are you defining?

- A. Network, and defining your Class A space
- B. Topology, and you are defining the Internal network
- C. Internal addresses you are defining the gateways
- D. Internal network(s) you are defining your networks

Answer: B

NEW QUESTION 149

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 150

There are 4 ways to use the Management API for creating host object with R80 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 155

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 158

When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of:

- A. Threat Emulation
- B. HTTPS
- C. QOS
- D. VoIP

Answer: D

NEW QUESTION 159

You have enabled “Full Log” as a tracking option to a security rule. However, you are still not seeing any data type information. What is the MOST likely reason?

- A. Logging has disk space issue
- B. Change logging storage options on the logging server or Security Management Server properties and install database.
- C. Data Awareness is not enabled.
- D. Identity Awareness is not enabled.
- E. Logs are arriving from Pre-R80 gateways.

Answer: A

NEW QUESTION 164

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 168

DLP and Geo Policy are examples of what type of Policy?

- A. Standard Policies
- B. Shared Policies
- C. Inspection Policies
- D. Unified Policies

Answer: B

NEW QUESTION 169

Check Point security components are divided into the following components:

- A. GUI Client, Security Gateway, WebUI Interface
- B. GUI Client, Security Management, Security Gateway
- C. Security Gateway, WebUI Interface, Consolidated Security Logs
- D. Security Management, Security Gateway, Consolidate Security Logs

Answer: B

NEW QUESTION 174

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 179

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 182

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 185

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 186

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 187

Which statement is true regarding redundancy?

- A. System Administrators know when their cluster has failed over and can also see why it failed over by using the cphaprob -f if command.
- B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
- C. Machines in a ClusterXL High Availability configuration must be synchronized.
- D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.

Answer: D

NEW QUESTION 192

CoreXL is supported when one of the following features is enabled:

- A. Route-based VPN
- B. IPS
- C. IPv6
- D. Overlapping NAT

Answer: B

Explanation:

CoreXL does not support Check Point Suite with these features: References:

NEW QUESTION 197

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 199

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 203

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 205

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 208

What is the purpose of the CPCA process?

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

Answer: D

NEW QUESTION 212

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 214

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 219

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

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

Answer: D

NEW QUESTION 221

By default, which port does the WebUI listen on?

- A. 80
- B. 4434
- C. 443
- D. 8080

Answer: C

NEW QUESTION 222

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 225

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 228

Which command is used to display status information for various components?

- A. show all systems
- B. show system messages
- C. sysmess all
- D. show sysenv all

Answer: D

NEW QUESTION 229

VPN Link Selection will perform the following when the primary VPN link goes down?

- A. The Firewall will drop the packets.
- B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.

- C. The Firewall will send out the packet on all interfaces.
- D. The Firewall will inform the client that the tunnel is down.

Answer: B

NEW QUESTION 230

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 235

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 239

Connections to the Check Point R80 Web API use what protocol?

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

Answer: A

NEW QUESTION 242

What is the recommended number of physical network interfaces in a Mobile Access cluster deployment?

- A. 4 Interfaces – an interface leading to the organization, a second interface leading to the internet, a third interface for synchronization, a fourth interface leading to the Security Management Server.
- B. 3 Interfaces – an interface leading to the organization, a second interface leading to the Internet, a third interface for synchronization.
- C. 1 Interface – an interface leading to the organization and the Internet, and configure for synchronization.
- D. 2 Interfaces – a data interface leading to the organization and the Internet, a second interface for synchronization.

Answer: B

NEW QUESTION 244

An administrator would like to troubleshoot why templating is not working for some traffic. How can he determine at which rule templating is disabled?

- A. He can use the fw accel stat command on the gateway.
- B. He can use the fw accel statistics command on the gateway.
- C. He can use the fwaccel stat command on the Security Management Server.
- D. He can use the fwaccel stat command on the gateway

Answer: D

NEW QUESTION 246

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 247

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 252

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

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

Answer: C

NEW QUESTION 257

What is the difference between an event and a log?

- A. Events are generated at gateway according to Event Policy
- B. A log entry becomes an event when it matches any rule defined in Event Policy
- C. Events are collected with SmartWorkflow form Trouble Ticket systems
- D. Log and Events are synonyms

Answer: B

NEW QUESTION 262

Tom has connected to the R80 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 266

Which is not a blade option when configuring SmartEvent?

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

Answer: B

Explanation:

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

NEW QUESTION 270

What is true about the IPS-Blade?

- A. In R80, IPS is managed by the Threat Prevention Policy
- B. In R80, in the IPS Layer, the only three possible actions are Basic, Optimized and Strict
- C. In R80, IPS Exceptions cannot be attached to "all rules"
- D. In R80, the GeoPolicy Exceptions and the Threat Prevention Exceptions are the same

Answer: A

NEW QUESTION 272

What API command below creates a new host with the name "New Host" and IP address of "192.168.0.10"?

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

Answer: D

NEW QUESTION 276

Which of the following statements is TRUE about R80 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 279

Which pre-defined Permission Profile should be assigned to an administrator that requires full access to audit all configurations without modifying them?

- A. Auditor
- B. Read Only All
- C. Super User
- D. Full Access

Answer: B

NEW QUESTION 284

Which CLI command will reset the IPS pattern matcher statistics?

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

Answer: D

NEW QUESTION 288

If an administrator wants to add manual NAT for addresses now owned by the Check Point firewall, what else is necessary to be completed for it to function properly?

- A. Nothing - the proxy ARP is automatically handled in the R80 version
- B. Add the proxy ARP configurations in a file called /etc/conf/local.arp
- C. Add the proxy ARP configurations in a file called \$FWDIR/conf/local.arp
- D. Add the proxy ARP configurations in a file called \$CPDIR/conf/local.arp

Answer: D

NEW QUESTION 292

Which method below is NOT one of the ways to communicate using the Management API's?

- A. Typing API commands using the "mgmt_cli" command
- B. Typing API commands from a dialog box inside the SmartConsole GUI application
- C. Typing API commands using Gaia's secure shell(clish)19+
- D. Sending API commands over an http connection using web-services

Answer: D

NEW QUESTION 297

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 302

Joey wants to upgrade from R75.40 to R80 version of Security management. He will use Advanced Upgrade with Database Migration method to achieve this. What is one of the requirements for his success?

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

Answer: B

NEW QUESTION 305

Using ClusterXL, what statement is true about the Sticky Decision Function?

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

Answer: A

NEW QUESTION 308

Which application should you use to install a contract file?

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

Answer: C

NEW QUESTION 313

Fill in the blank: The R80 utility fw monitor is used to troubleshoot _____ .

- A. User data base corruption
- B. LDAP conflicts
- C. Traffic issues
- D. Phase two key negotiations

Answer: C

Explanation:

Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark.

NEW QUESTION 314

When installing a dedicated R80 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 315

What is not a component of Check Point SandBlast?

- A. Threat Emulation
- B. Threat Simulator
- C. Threat Extraction
- D. Threat Cloud

Answer: B

NEW QUESTION 318

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 322

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 324

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 325

Which Check Point software blade provides protection from zero-day and undiscovered threats?

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

Answer: B

NEW QUESTION 326

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 329

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 supported
- E. So, if you wanted to employ Virtual Routers instead, you have to reconsider your design.

Answer: A

NEW QUESTION 331

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 333

Fill in the blank: The IPS policy for pre-R80 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/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 338

How can SmartView application accessed?

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

Answer: C

NEW QUESTION 339

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

- A. Dropped without sending a negative acknowledgment

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

Answer: D

NEW QUESTION 343

You have existing dbedit scripts from R77. Can you use them with R80.10?

- A. dbedit is not supported in R80.10
- B. dbedit is fully supported in R80.10
- 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 R80.10

Answer: D

NEW QUESTION 347

Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 352

.....

Relate Links

100% Pass Your 156-315.80 Exam with Exambible Prep Materials

<https://www.exambible.com/156-315.80-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/>