



Check-Point

Exam Questions 156-315.80

Check Point Certified Security Expert - R80

NEW QUESTION 1

Which of the SecureXL templates are enabled by default on Security Gateway?

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

Answer: D

NEW QUESTION 2

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 3

What is the default size of NAT table fw_x_alloc?

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

Answer: C

NEW QUESTION 4

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 5

Which configuration file contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status?

- A. \$FWDIR/database/fwauthd.conf
- B. \$FWDIR/conf/fwauth.conf
- C. \$FWDIR/conf/fwauthd.conf
- D. \$FWDIR/state/fwauthd.conf

Answer: C

NEW QUESTION 6

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 7

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 8

Which blades and or features are not supported in R80?

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

Answer: A

NEW QUESTION 9

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

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 10

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 13

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 16

The SmartEvent R80 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 18

Which of the following is NOT a type of Endpoint Identity Agent?

- A. Terminal
- B. Light
- C. Full
- D. Custom

Answer: A

NEW QUESTION 23

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 24

What statement best describes the Proxy ARP feature for Manual NAT in R80.10?

- 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 29

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

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

Answer: D

NEW QUESTION 34

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 36

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

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

Answer: B

NEW QUESTION 40

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 44

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 49

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 52

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 54

You can access the ThreatCloud Repository from:

- A. R80.10 SmartConsole and Application Wiki
- B. Threat Prevention and Threat Tools
- C. Threat Wiki and Check Point Website
- D. R80.10 SmartConsole and Threat Prevention

Answer: D

NEW QUESTION 59

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 61

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 64

What are the two high availability modes?

- A. Load Sharing and Legacy
- B. Traditional and New
- C. Active and Standby
- D. New and Legacy

Answer: D

Explanation:

ClusterXL has four working modes. This section briefly describes each mode and its relative advantages and disadvantages.

NEW QUESTION 66

Which is NOT an example of a Check Point API?

- A. Gateway API
- B. Management API
- C. OPSC SDK
- D. Threat Prevention API

Answer: A

NEW QUESTION 69

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 70

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 72

Which statement is correct about the Sticky Decision Function?

- A. It is not supported with either the Performance pack or a hardware based accelerator card
- B. Does not support SPI's when configured for Load Sharing
- C. It is automatically disabled if the Mobile Access Software Blade is enabled on the cluster
- D. It is not required for L2TP traffic

Answer: A

NEW QUESTION 75

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 78

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 81

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 83

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 85

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 89

Which GUI client is supported in R80?

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

Answer: C

NEW QUESTION 92

Which TCP-port does CPM process listen to?

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

Answer: D

NEW QUESTION 93

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 98

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 100

Which process handles connection from SmartConsole R80?

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

Answer: C

NEW QUESTION 105

Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links.

Which component of SandBlast protection is her company using on a Gateway?

- A. SandBlast Threat Emulation
- B. SandBlast Agent
- C. Check Point Protect
- D. SandBlast Threat Extraction

Answer: D

NEW QUESTION 108

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 110

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 112

You are asked to check the status of several user-mode processes on the management server and gateway. Which of the following processes can only be seen on a Management Server?

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

Answer: B

NEW QUESTION 115

John is using Management HA. Which Smartcenter should be connected to for making changes?

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

Answer: B

NEW QUESTION 118

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 123

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

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

Answer: C

NEW QUESTION 127

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 130

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 131

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 132

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 134

What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 138

You have successfully backed up Check Point configurations without the OS information. What command would you use to restore this backup?

- A. restore_backup
- B. import backup
- C. cp_merge
- D. migrate import

Answer: D

NEW QUESTION 140

What component of R80 Management is used for indexing?

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

Answer: D

NEW QUESTION 142

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 145

On R80.10 when configuring Third-Party devices to read the logs using the LEA (Log Export API) the default Log Server uses port:

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

Answer: B

NEW QUESTION 150

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 154

On R80.10 the IPS Blade is managed by:

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

Answer: C

NEW QUESTION 156

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 158

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 159

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 161

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 164

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 169

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 170

Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAi/R80.10. 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 173

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 174

Fill in the blank: A new license should be generated and installed in all of the following situations EXCEPT when _____ .

- A. The license is attached to the wrong Security Gateway.
- B. The existing license expires.
- C. The license is upgraded.
- D. The IP address of the Security Management or Security Gateway has changed.

Answer: A

NEW QUESTION 176

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 177

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 178

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 183

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?

- 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 185

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 186

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 189

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 192

What is the default shell for the command line interface?

- A. Expert
- B. Clish
- C. Admin
- D. Normal

Answer: B

Explanation:

The default shell of the CLI is called clish

NEW QUESTION 194

What does the Log "Views" tab show when SmartEvent is Correlating events?

- A. A list of common reports
- B. Reports for customization
- C. Top events with charts and graphs
- D. Details of a selected logs

Answer: C

NEW QUESTION 198

What is the command to see cluster status in cli expert mode?

- A. fw ctl stat
- B. clusterXL stat
- C. clusterXL status
- D. cphaprob stat

Answer: D

NEW QUESTION 202

SmartEvent does NOT use which of the following procedures to identify events:

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

Answer: C

Explanation:

Events are detected by the SmartEvent Correlation Unit. The Correlation Unit task is to scan logs for criteria that match an Event Definition. SmartEvent uses these procedures to identify events:

- Matching a Log Against Global Exclusions
- Matching a Log Against Each Event Definition
- Creating an Event Candidate
- When a Candidate Becomes an Event References:

NEW QUESTION 203

In what way are SSL VPN and IPSec VPN different?

- A. SSL VPN is using HTTPS in addition to IKE, whereas IPSec VPN is clientless
- B. SSL VPN adds an extra VPN header to the packet, IPSec VPN does not
- C. IPSec VPN does not support two factor authentication, SSL VPN does support this
- D. IPSec VPN uses an additional virtual adapter; SSL VPN uses the client network adapter only.

Answer: D

NEW QUESTION 208

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 Connectoffers 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 211

What is considered Hybrid Emulation Mode?

- A. Manual configuration of file types on emulation location.

- B. Load sharing of emulation between an on premise appliance and the cloud.
- C. Load sharing between OS behavior and CPU Level emulation.
- D. High availability between the local SandBlast appliance and the cloud.

Answer: B

NEW QUESTION 216

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 219

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated management console. It empowers the migration from legacy Client-side logic to Server-side logic. The cpm process:

- A. Allow GUI Client and management server to communicate via TCP Port 19001
- B. Allow GUI Client and management server to communicate via TCP Port 18191
- C. Performs database tasks such as creating, deleting, and modifying objects and compiling policy.
- D. Performs database tasks such as creating, deleting, and modifying objects and compiling as well as policy code generation.

Answer: C

NEW QUESTION 222

In the R80 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 227

Which is NOT a SmartEvent component?

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

Answer: C

NEW QUESTION 231

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 233

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 234

One of major features in R80 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 235

To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

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

Answer: B

NEW QUESTION 236

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 240

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 244

What are the attributes that SecureXL will check after the connection is allowed by Security Policy?

- A. Source address, Destination address, Source port, Destination port, Protocol
- B. Source MAC address, Destination MAC address, Source port, Destination port, Protocol
- C. Source address, Destination address, Source port, Destination port
- D. Source address, Destination address, Destination port, Protocol

Answer: A

NEW QUESTION 249

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 250

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 251

Which remote Access Solution is clientless?

- A. Checkpoint Mobile
- B. Endpoint Security Suite
- C. SecuRemote
- D. Mobile Access Portal

Answer: D

NEW QUESTION 253

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

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

Answer: C

NEW QUESTION 256

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 261

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 264

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 266

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 270

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 275

In which formats can Threat Emulation forensics reports be viewed in?

- A. TXT, XML and CSV
- B. PDF and TXT
- C. PDF, HTML, and XML
- D. PDF and HTML

Answer: C

NEW QUESTION 280

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 284

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 288

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 290

What is the purpose of a SmartEvent Correlation Unit?

- A. The SmartEvent Correlation Unit is designed to check the connection reliability from SmartConsole to the SmartEvent Server.
- B. The SmartEvent Correlation Unit's task is to assign severity levels to the identified events.
- C. The Correlation unit role is to evaluate logs from the log server component to identify patterns/threats and convert them to events.
- D. The SmartEvent Correlation Unit is designed to check the availability of the SmartReporter Server.

Answer: C

NEW QUESTION 293

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 295

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 296

In the Firewall chain mode FFF refers to:

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

Answer: C

NEW QUESTION 299

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 300

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 301

Which is the least ideal Synchronization Status for Security Management Server High Availability deployment?

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

Answer: D

NEW QUESTION 305

Both ClusterXL and VRRP are fully supported by Gaia R80.10 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 308

Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 313

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 318

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 322

What are the blades of Threat Prevention?

- A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
- B. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
- C. IPS, AntiVirus, AntiBot
- D. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction

Answer: D

NEW QUESTION 325

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 327

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 330

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

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

Answer: B

NEW QUESTION 334

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 336

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 338

The following command is used to verify the CPUSE version:

- A. HostName:0>show installer status build
- B. [Expert@HostName:0]#show installer status
- C. [Expert@HostName:0]#show installer status build
- D. HostName:0>show installer build

Answer: A

NEW QUESTION 342

Which one of the following is true about Capsule Connect?

- A. It is a full layer 3 VPN client
- B. It offers full enterprise mobility management
- C. It is supported only on iOS phones and Windows PCs
- D. It does not support all VPN authentication methods

Answer: A

NEW QUESTION 344

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 348

Which view is NOT a valid CPVIEW view?

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

Answer: C

NEW QUESTION 353

Sieve is a Cyber Security Engineer working for Global Bank with a large scale deployment of Check Point Enterprise Appliances Steve's manager. Diana asks him to provide firewall connection table details from one of the firewalls for which he is responsible. Which of these commands may impact performance briefly and should not be used during heavy traffic times of day?

- A. fw tab -t connections -s
- B. fw tab -t connections
- C. fw tab -t connections -c
- D. fw tab -t connections -f

Answer: B

NEW QUESTION 358

Which directory below contains log files?

- A. /opt/CPSmartlog-R80/log
- B. /opt/CPshrd-R80/log
- C. /opt/CPsuite-R80/fw1/log
- D. /opt/CPsuite-R80/log

Answer: C

NEW QUESTION 361

How do Capsule Connect and Capsule Workspace differ?

- A. Capsule Connect provides a Layer3 VP
- B. Capsule Workspace provides a Desktop with usable applications.
- C. Capsule Workspace can provide access to any application.
- D. Capsule Connect provides Business data isolation.
- E. Capsule Connect does not require an installed application at client.

Answer: A

NEW QUESTION 364

Which SmartConsole tab is used to monitor network and security performance?

- A. Manage Setting
- B. Security Policies
- C. Gateway and Servers
- D. Logs and Monitor

Answer: D

NEW QUESTION 365

You have existing dcredit 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 370

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

156-315.80 Practice Exam Features:

- * 156-315.80 Questions and Answers Updated Frequently
- * 156-315.80 Practice Questions Verified by Expert Senior Certified Staff
- * 156-315.80 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 156-315.80 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 156-315.80 Practice Test Here](#)