



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

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: B

NEW QUESTION 3

In the Check Point Firewall Kernel Module, each Kernel is associated with a key, which specifies the type of traffic applicable to the chain module. For Wire Mode configuration, chain modules marked with _____ will not apply.

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

Answer: B

NEW QUESTION 4

To help SmartEvent determine whether events originated internally or externally you must define using the Initial Settings under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?

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

Answer: D

NEW QUESTION 5

In a Client to Server scenario, which represents that the packet has already checked against the tables and the Rule Base?

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

Answer: D

NEW QUESTION 6

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 7

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 8

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 9

What is the minimum amount of RAM needed for a Threat Prevention Appliance?

- A. 6 GB
- B. 8GB with Gaia in 64-bit mode
- C. 4 GB
- D. It depends on the number of software blades enabled

Answer: C

NEW QUESTION 10

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 10

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 15

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 19

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 23

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 27

Which one of the following is true about Threat Emulation?

- A. Takes less than a second to complete
- B. Works on MS Office and PDF files only
- C. Always delivers a file
- D. Takes minutes to complete (less than 3 minutes)

Answer: D

NEW QUESTION 32

When attempting to start a VPN tunnel, in the logs the error “no proposal chosen” is seen numerous times. No other VPN-related entries are present. Which phase of the VPN negotiations has failed?

- A. IKE Phase 1
- B. IPSEC Phase 2
- C. IPSEC Phase 1
- D. IKE Phase 2

Answer: A

NEW QUESTION 36

What is the correct order of the default “fw monitor” inspection points?

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

Answer: C

NEW QUESTION 40

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 44

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 48

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 49

What is the most ideal Synchronization Status for Security Management Server High Availability deployment?

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

Answer: B

NEW QUESTION 52

Which of the following Check Point processes within the Security Management Server is responsible for the receiving of log records from Security Gateway?

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

Answer: B

NEW QUESTION 54

Which of the following is NOT a type of Check Point API available in R80.10?

- A. Identity Awareness Web Services
- B. OPSEC SDK
- C. Mobile Access
- D. Management

Answer: C

NEW QUESTION 57

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 58

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 61

When users connect to the Mobile Access portal they are unable to open File Shares. Which log file would you want to examine?

- A. cvpnd.elg
- B. httpd.elg
- C. vpnd.elg
- D. fw.elg

Answer: A

NEW QUESTION 63

As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

- A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
- B. Full Layer4 VPN –SSL VPN that gives users network access to all mobile applications.
- C. Full Layer3 VPN –IPSec VPN that gives users network access to all mobile applications.
- D. You can make sure that documents are sent to the intended recipients only.

Answer: C

NEW QUESTION 66

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 71

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 74

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 78

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 82

What needs to be configured if the NAT property 'Translate destination or client side' is not enabled in Global Properties?

- A. A host route to route to the destination IP.
- B. Use the file local.arp to add the ARP entries for NAT to work.
- C. Nothing, the Gateway takes care of all details necessary.
- D. Enabling 'Allow bi-directional NAT' for NAT to work correctly.

Answer: C

NEW QUESTION 87

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: C

NEW QUESTION 88

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 93

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 94

Which Check Point feature enables application scanning and the detection?

- A. Application Dictionary
- B. AppWiki
- C. Application Library
- D. CPApp

Answer: B

NEW QUESTION 96

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 101

What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 103

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 108

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 110

Which is NOT an example of a Check Point API?

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

Answer: A

NEW QUESTION 111

What component of R80 Management is used for indexing?

- A. DBSync

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

Answer: D

NEW QUESTION 113

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 116

How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

- A. cphaprob set int fwha_vmac_global_param_enabled 1
- B. clusterXL set int fwha_vmac_global_param_enabled 1
- C. fw ctl set int fwha_vmac_global_param_enabled 1
- D. cphaconf set int fwha_vmac_global_param_enabled 1

Answer: C

NEW QUESTION 120

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 124

GAiA Software update packages can be imported and installed offline in situation where:

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

Answer: B

NEW QUESTION 125

Which statement is most correct regarding about "CoreXL Dynamic Dispatcher"?

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

Answer: B

NEW QUESTION 129

How many policy layers do Access Control policy support?

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

Answer: A

Explanation:

Two policy layers:

- Network Policy Layer
- Application Control Policy Layer

NEW QUESTION 131

Identify the API that is not supported by Check Point currently.

- A. R80 Management API-
- B. Identity Awareness Web Services API
- C. Open REST API
- D. OPSEC SDK

Answer: C

NEW QUESTION 133

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 136

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 139

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 142

Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

- A. Application Control
- B. Threat Emulation
- C. Anti-Virus
- D. Advanced Networking Blade

Answer: B

NEW QUESTION 143

What is the limitation of employing Sticky Decision Function?

- A. With SDF enabled, the involved VPN Gateways only supports IKEv1
- B. Acceleration technologies, such as SecureXL and CoreXL are disabled when activating SDF
- C. With SDF enabled, only ClusterXL in legacy mode is supported
- D. With SDF enabled, you can only have three Sync interfaces at most

Answer: B

NEW QUESTION 148

Which encryption algorithm is the least secured?

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

Answer: C

NEW QUESTION 152

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 154

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 159

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 161

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 163

When running a query on your logs, to find records for user Toni with machine IP of 10.0.4.210 but exclude her tablet IP of 10.0.4.76, which of the following query syntax would you use?

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

Answer: B

NEW QUESTION 168

What key is used to save the current CPView page in a filename format cpview_”cpview process ID”.cap”number of captures”?

- A. S
- B. W
- C. C
- D. Space bar

Answer: C

NEW QUESTION 170

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 173

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 175

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 179

To fully enable Dynamic Dispatcher with Firewall Priority Queues on a Security Gateway, run the following command in Expert mode then reboot:

- A. fw ctl multik set_mode 1
- B. fw ctl Dynamic_Priority_Queue on
- C. fw ctl Dynamic_Priority_Queue enable
- D. fw ctl multik set_mode 9

Answer: D

NEW QUESTION 181

Which Check Point software blade provides Application Security and identity control?

- A. Identity Awareness
- B. Data Loss Prevention
- C. URL Filtering
- D. Application Control

Answer: D

NEW QUESTION 182

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

Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or via CLI. Which command should he use in CLI? (Choose the correct answer.)

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

Answer: D

NEW QUESTION 190

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 194

What SmartEvent component creates events?

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

Answer: B

NEW QUESTION 198

Advanced Security Checkups can be easily conducted within:

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

Answer: A

NEW QUESTION 202

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 207

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 210

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 212

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 216

Fill in the blank: The tool _____ generates a R80 Security Gateway configuration report.

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

Answer: C

NEW QUESTION 217

When setting up an externally managed log server, what is one item that will not be configured on the R80 Security Management Server?

- A. IP
- B. SIC
- C. NAT
- D. FQDN

Answer: C

NEW QUESTION 219

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 222

Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?

- A. The rule base can be built of layers, each containing a set of the security rule
- B. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
- C. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
- D. Time object to a rule to make the rule active only during specified times.
- E. Sub Policies are sets of rules that can be created and attached to specific rule
- F. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule.

Answer: D

NEW QUESTION 225

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 226

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 228

By default, which port does the WebUI listen on?

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

Answer: C

NEW QUESTION 232

The _____ software blade package uses CPU-level and OS-level sandboxing in order to detect and block malware.

- A. Next Generation Threat Prevention
- B. Next Generation Threat Emulation
- C. Next Generation Threat Extraction
- D. Next Generation Firewall

Answer: B

NEW QUESTION 236

What cloud-based SandBlast Mobile application is used to register new devices and users?

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

Answer: D

NEW QUESTION 240

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 244

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 245

Which of the following is NOT an option to calculate the traffic direction?

- A. Incoming
- B. Internal
- C. External
- D. Outgoing

Answer: D

NEW QUESTION 248

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 249

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 253

When requiring certificates for mobile devices, make sure the authentication method is set to one of the following, Username and Password, RADIUS or _____.

- A. SecureID
- B. SecurID
- C. Complexity
- D. TacAcs

Answer: B

NEW QUESTION 257

When SecureXL is enabled, all packets should be accelerated, except packets that match the following conditions:

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

Answer: D

NEW QUESTION 262

Automatic affinity means that if SecureXL is running, the affinity for each interface is automatically reset every

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

Answer: B

NEW QUESTION 264

Which tool is used to enable ClusterXL?

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

Answer: B

NEW QUESTION 266

Which of these is an implicit MEP option?

- A. Primary-backup
- B. Source address based
- C. Round robin
- D. Load Sharing

Answer: A

NEW QUESTION 269

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 271

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 276

How is communication between different Check Point components secured in R80? As with all questions, select the BEST answer.

- A. By using IPSEC
- B. By using SIC
- C. By using ICA
- D. By using 3DES

Answer: B

NEW QUESTION 281

How many layers make up the TCP/IP model?

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

Answer: D

NEW QUESTION 286

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 287

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 291

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 293

What is the default shell of Gaia CLI?

- A. Monitor
- B. CLI.sh
- C. Read-only
- D. Bash

Answer: B

NEW QUESTION 295

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 296

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 298

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 299

If you needed the Multicast MAC address of a cluster, what command would you run?

- A. cphaprob -a if
- B. cphaconf ccp multicast
- C. cphaconf debug data
- D. cphaprob igmp

Answer: D

NEW QUESTION 302

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 305

What Factor preclude Secure XL Templating?

- A. Source Port Ranges/Encrypted Connections
- B. IPS
- C. ClusterXL in load sharing Mode
- D. CoreXL

Answer: A

NEW QUESTION 309

What are the main stages of a policy installations?

- A. Verification & Compilation, Transfer and Commit
- B. Verification & Compilation, Transfer and Installation
- C. Verification, Commit, Installation
- D. Verification, Compilation & Transfer, Installation

Answer: B

NEW QUESTION 313

Office mode means that:

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

Answer: D

NEW QUESTION 314

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 317

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 318

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 323

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 326

Where you can see and search records of action done by R80 SmartConsole administrators?

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

Answer: B

NEW QUESTION 329

SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

- A. Smart Cloud Services
- B. Load Sharing Mode Services
- C. Threat Agent Solution
- D. Public Cloud Services

Answer: A

NEW QUESTION 330

Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 333

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 337

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 342

Which NAT rules are prioritized first?

- A. Post-Automatic/Manual NAT rules
- B. Manual/Pre-Automatic NAT
- C. Automatic Hide NAT
- D. Automatic Static NAT

Answer: B

NEW QUESTION 345

Fill in the blank: The R80 SmartConsole, SmartEvent GUI client, and _____ consolidate billions of logs and shows them as prioritized security events.

- A. SmartMonitor
- B. SmartView Web Application
- C. SmartReporter
- D. SmartTracker

Answer: B

NEW QUESTION 350

The following command is used to verify the CPUISE 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 354

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 355

Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidated 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 359

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 361

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 362

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 363

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 368

.....

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](#)