

Check-Point

Exam Questions 156-315.80

Check Point Certified Security Expert - R80



NEW QUESTION 1

The fwd process on the Security Gateway sends logs to the fwd process on the Management Server via which 2 processes?

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

Answer: A

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

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 4

How many interfaces can you configure to use the Multi-Queue feature?

- A. 10 interfaces
- B. 3 interfaces
- C. 4 interfaces
- D. 5 interfaces

Answer: D

Explanation:

Note - References:

NEW QUESTION 5

In terms of Order Rule Enforcement, when a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom Which of the following statements is correct?

- A. If the Action of the matching rule is Accept the gateway will drop the packet
- B. If the Action of the matching rule is Drop, the gateway continues to check rules in the next Policy Layer down
- C. If the Action of the matching rule is Drop the gateway stops matching against later rules in the Policy Rule Base and drops the packet
- D. If the rule does not matched in the Network policy it will continue to other enabled polices

Answer: C

Explanation:

https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_

NEW QUESTION 6

After making modifications to the \$CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?

- A. cvpnd_restart
- B. cvpnd_restart
- C. cvpnd restart
- D. cvpnrestart

Answer: B

NEW QUESTION 7

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 8

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 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

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

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

Answer: A

NEW QUESTION 10

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 13

What is the valid range for VRID value in VRRP configuration?

- A. 1 - 254
- B. 1 - 255
- C. 0 - 254
- D. 0 - 255

Answer: B

Explanation:

Virtual Router ID - Enter a unique ID number for this virtual router. The range of valid values is 1 to 255. \

NEW QUESTION 15

What are the different command sources that allow you to communicate with the API server?

- A. SmartView Monitor, API_cli Tool, Gaia CLI, Web Services
- B. SmartConsole GUI Console, mgmt_cli Tool, Gaia CLI, Web Services
- C. SmartConsole GUI Console, API_cli Tool, Gaia CLI, Web Services
- D. API_cli Tool, Gaia CLI, Web Services

Answer: B

NEW QUESTION 19

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 23

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 26

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 30

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 31

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 36

You plan to automate creating new objects using new R80 Management API. You decide to use GAIA CLI for this task. What is the first step to run management API commands on GAIA's shell?

- A. mgmt_admin@teabag > id.txt
- B. mgmt_login
- C. login user admin password teabag
- D. mgmt_cli login user "admin" password "teabag" > id.txt

Answer: B

NEW QUESTION 40

You need to change the number of firewall Instances used by CoreXL. How can you achieve this goal?

- A. edit fwaffinity.conf; reboot required
- B. cpconfig; reboot required
- C. edit fwaffinity.conf; reboot not required
- D. cpconfig; reboot not required

Answer: B

NEW QUESTION 43

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 47

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 51

What processes does CPM control?

- A. Object-Store, Database changes, CPM Process and web-services
- B. web-services, CPML 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 55

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 60

Check Point recommends configuring Disk Space Management parameters to delete old log entries when available disk space is less than or equal to?

- A. 50%
- B. 75%
- C. 80%
- D. 15%

Answer: D

NEW QUESTION 63

During inspection of your Threat Prevention logs you find four different computers having one event each with a Critical Severity. Which of those hosts should you try to remediate first?

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

Answer: D

NEW QUESTION 67

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 71

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 72

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 74

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 76

When a packet arrives at the gateway, the gateway checks it against the rules in the hop Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet. Which of the following statements about the order of rule enforcement is true?

- A. If the Action is Accept, the gateway allows the packet to pass through the gateway.
- B. If the Action is Drop, the gateway continues to check rules in the next Policy Layer down.
- C. If the Action is Accept, the gateway continues to check rules in the next Policy Layer down.
- D. If the Action is Drop, the gateway applies the Implicit Clean-up Rule for that Policy Layer.

Answer: C

NEW QUESTION 79

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 83

Which process handles connection from SmartConsole R80?

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

Answer: C

NEW QUESTION 88

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 89

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 93

What is the purpose of Priority Delta in VRRP?

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

Answer: C

Explanation:

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

NEW QUESTION 94

Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

- A. Detects and blocks malware by correlating multiple detection engines before users are affected.
- B. Configure rules to limit the available network bandwidth for specified users or groups.
- C. Use UserCheck to help users understand that certain websites are against the company's security policy.
- D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A

NEW QUESTION 99

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 102

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 107

An administrator is creating an IPsec site-to-site VPN between his corporate office and branch office. Both offices are protected by Check Point Security Gateway managed by the same Security Management Server. While configuring the VPN community to specify the pre-shared secret the administrator found that the check box to enable pre-shared secret and cannot be enabled.

Why does it not allow him to specify the pre-shared secret?

- A. IPsec VPN blade should be enabled on both Security Gateway.
- B. Pre-shared can only be used while creating a VPN between a third party vendor and Check Point Security Gateway.
- C. Certificate based Authentication is the only authentication method available between two Security Gateway managed by the same SMS.
- D. The Security Gateways are pre-R75.40.

Answer: C

NEW QUESTION 112

Fill in the blanks: Gaia can be configured using the _____ or _____.

- A. GaiaUI; command line interface
- B. WebUI; Gaia Interface
- C. Command line interface; WebUI
- D. Gaia Interface; GaiaUI

Answer: C

NEW QUESTION 117

Vanessa is firewall administrator in her company. Her company is using Check Point firewall on a central and several remote locations which are managed centrally by R77.30 Security Management Server. On central location is installed R77.30 Gateway on Open server. Remote locations are using Check Point UTM-1570 series appliances with R75.30 and some of them are using a UTM-1-Edge-X or Edge-W with latest available firmware. She is in process of migrating to R80.

What can cause Vanessa unnecessary problems, if she didn't check all requirements for migration to R80?

- A. Missing an installed R77.20 Add-on on Security Management Server
- B. Unsupported firmware on UTM-1 Edge-W appliance
- C. Unsupported version on UTM-1 570 series appliance
- D. Unsupported appliances on remote locations

Answer: A

NEW QUESTION 121

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 122

True or False: In R80, more than one administrator can login to the Security Management Server with write permission at the same time.

- A. False, this feature has to be enabled in the Global Properties.
- B. True, every administrator works in a session that is independent of the other administrators.
- C. True, every administrator works on a different database that is independent of the other administrators.
- D. False, only one administrator can login with write permission.

Answer: B

NEW QUESTION 126

What are the three components for Check Point Capsule?

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

Answer: D

NEW QUESTION 127

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 128

Which Mobile Access Application allows a secure container on Mobile devices to give users access to internal website, file share and emails?

- A. Check Point Remote User
- B. Check Point Capsule Workspace
- C. Check Point Mobile Web Portal
- D. Check Point Capsule Remote

Answer: C

NEW QUESTION 132

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 136

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 138

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 139

Which web services protocol is used to communicate to the Check Point R80 Identity Awareness Web API?

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

Answer: B

Explanation:

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

NEW QUESTION 141

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 146

SmartEvent uses it's event policy to identify events. How can this be customized?

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

Answer: C

NEW QUESTION 151

Which options are given on features, when editing a Role on Gaia Platform?

- A. Read/Write, Read Only
- B. Read/Write, Read Only, None
- C. Read/Write, None
- D. Read Only, None

Answer: B

NEW QUESTION 152

What is the main difference between Threat Extraction and Threat Emulation?

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

Answer: B

NEW QUESTION 157

On what port does the CPM process run?

- A. TCP 857
- B. TCP 18192
- C. TCP 900
- D. TCP 19009

Answer: D

NEW QUESTION 158

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 161

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 162

Vanessa is a Firewall administrator. She wants to test a backup of her company's production Firewall cluster Dallas_GW. She has a lab environment that is identical to her production environment. She decided to restore production backup via SmartConsole in lab environment. Which details she need to fill in System Restore window before she can click OK button and test the backup?

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

Answer: C

NEW QUESTION 167

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 168

Fill in the blank: The command _____ provides the most complete restoration of a R80 configuration.

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

Answer: A

NEW QUESTION 169

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 170

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 172

In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

- A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
- B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
- C. Mail, Block Source, Block Destination, External Script, SNMP Trap
- D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Answer: A

NEW QUESTION 177

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 180

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 185

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 190

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 192

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 194

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 197

Which command will allow you to see the interface status?

- A. cphaprob interface
- B. cphaprob -l interface
- C. cphaprob -a if
- D. cphaprob stat

Answer: C

NEW QUESTION 202

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 203

Which two of these Check Point Protocols are used by SmartEvent Processes?

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

Answer: D

NEW QUESTION 204

Tom has been tasked to install Check Point R80 in a distributed deployment. Before Tom installs the systems this way, how many machines will he need if he does NOT include a SmartConsole machine in his calculations?

- A. One machine, but it needs to be installed using SecurePlatform for compatibility purposes.
- B. One machine
- C. Two machines
- D. Three machines

Answer: C

Explanation:

One for Security Management Server and the other one for the Security Gateway.

NEW QUESTION 205

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 207

How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

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

Answer: C

NEW QUESTION 208

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 209

Which tool provides a list of trusted files to the administrator so they can specify to the Threat Prevention blade that these files do not need to be scanned or analyzed?

- A. ThreatWiki
- B. Whitelist Files
- C. AppWiki
- D. IPS Protections

Answer: B

NEW QUESTION 212

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 215

When simulating a problem on ClusterXL cluster with `cphaprob -d STOP -s problem -t 0 register`, to initiate a failover on an active cluster member, what command allows you remove the problematic state?

- A. `cphaprob -d STOP unregister`
- B. `cphaprob STOP unregister`
- C. `cphaprob unregister STOP`
- D. `cphaprob -d unregister STOP`

Answer: A

Explanation:

esting a failover in a controlled manner using following command;

```
# cphaprob -d STOP -s problem -t 0 register
```

This will register a problem state on the cluster member this was entered on; If you then run;

```
# cphaprob list
```

this will show an entry named STOP.

to remove this problematic register run following;

```
# cphaprob -d STOP unregister
```

 References:

NEW QUESTION 216

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 218

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 219

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 224

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 229

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 233

With SecureXL enabled, accelerated packets will pass through the following:

- A. Network Interface Card, OSI Network Layer, OS IP Stack, and the Acceleration Device
- B. Network Interface Card, Check Point Firewall Kernel, and the Acceleration Device
- C. Network Interface Card and the Acceleration Device
- D. Network Interface Card, OSI Network Layer, and the Acceleration Device

Answer: C

NEW QUESTION 238

Which command is used to set the CCP protocol to Multicast?

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

Answer: B

NEW QUESTION 240

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 243

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 from Trouble Ticket systems
- D. Log and Events are synonyms

Answer: B

NEW QUESTION 246

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 247

What is the valid range for Virtual Router Identifier (VRID) value in a Virtual Routing Redundancy Protocol (VRRP) configuration?

- A. 1-254
- B. 1-255
- C. 0-254
- D. 0 – 255

Answer: B

NEW QUESTION 249

What is the default shell of Gaia CLI?

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

Answer: B

NEW QUESTION 252

Which command collects diagnostic data for analyzing customer setup remotely?

- A. cpinfo
- B. migrate export
- C. sysinfo
- D. cpview

Answer: A

Explanation:

CPInfo is an auto-updatable utility that collects diagnostics data on a customer's machine at the time of execution and uploads it to Check Point servers (it replaces the standalone cp_uploader utility for uploading files to Check Point servers).

The CPInfo output file allows analyzing customer setups from a remote location. Check Point support engineers can open the CPInfo file in a demo mode, while viewing actual customer Security Policies and Objects. This allows the in-depth analysis of customer's configuration and environment settings.

NEW QUESTION 257

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 262

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 266

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 269

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 274

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 278

Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 282

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 287

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 292

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 294

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 298

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 301

Which view is NOT a valid CPVIEW view?

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

Answer: C

NEW QUESTION 305

Which of the following authentication methods ARE NOT used for Mobile Access?

- A. RADIUS server
- B. Username and password (internal, LDAP)
- C. SecurID
- D. TACACS+

Answer: D

NEW QUESTION 309

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 314

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 318

In Logging and Monitoring, the tracking options are Log, Detailed Log and Extended Log. Which of the following options can you add to each Log, Detailed Log and Extended Log?

- A. Accounting
- B. Suppression
- C. Accounting/Suppression
- D. Accounting/Extended

Answer: C

NEW QUESTION 320

.....

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](#)