Check-Point

Exam Questions 156-315.80

Check Point Certified Security Expert - R80

NEW QUESTION 1
Which Check Point software blades could be enforced under Threat Prevention profile using Check Point R80.10 SmartConsole application?

A. IPS, Anti-Bot, URL Filtering, Application Control, Threat Emulation.
B. Firewall, IPS, Threat Emulation, Application Control.
C. IPS, Anti-Bot, Anti-Virus, Threat Emulation, Threat Extraction.
D. Firewall, IPS, Anti-Bot, Anti-Virus, Threat Emulation.

Answer: C

NEW QUESTION 2
Which of the SecureXL templates are enabled by default on Security Gateway?

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

Answer: D

NEW QUESTION 3
What happen when IPS profile is set in Detect Only Mode for troubleshooting?

A. It will generate Geo-Protection traffic
B. Automatically uploads debugging logs to Check Point Support Center
C. It will not block malicious traffic
D. Bypass licenses requirement for Geo-Protection control

Answer: C

Explanation:
It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic.
During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic.

NEW QUESTION 4
What is the recommended configuration when the customer requires SmartLog indexing for 14 days and SmartEvent to keep events for 180 days?

A. Use Multi-Domain Management Server.
B. Choose different setting for log storage and SmartEvent db
C. Install Management and SmartEvent on different machines.
D. it is not possible.

Answer: B

NEW QUESTION 5
Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs
B. Capsule Cloud
C. Capsule Enterprise
D. Capsule Workspace

Answer: C

NEW QUESTION 6
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 7
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 8
What is the default size of NAT table fwx_alloc?

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

Answer: C

NEW QUESTION 9
From SecureXL perspective, what are the tree paths of traffic flow:

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

Answer: D

NEW QUESTION 10
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 10
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 14
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 18
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 22
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 24
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 28
Please choose correct command to add an “emailserver1” host with IP address 10.50.23.90 using GAiA management CLI?

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

Answer: D

NEW QUESTION 32
Which of the following Windows Security Events will not map a username to an IP address in Identity Awareness?

A. Kerberos Ticket Renewed
B. Kerberos Ticket Requested
C. Account Logon
D. Kerberos Ticket Timed Out

Answer: D

NEW QUESTION 35
Which of the following is NOT a type of Endpoint Identity Agent?

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

Answer: A

NEW QUESTION 39
The essential means by which state synchronization works to provide failover in the event an active member goes down, _______ is used specifically for clustered environments to allow gateways to report their own state and learn about the states of other members in the cluster.

A. ccp
B. cphaconf
C. cphad
D. cphastart

Answer: A

NEW QUESTION 42
SmartEvent provides a convenient way to run common command line executables that can assist in investigating events. Right-clicking the IP address, source or destination, in an event provides a list of default and customized commands. They appear only on cells that refer to IP addresses because the IP address of the active cell is used as the destination of the command when run. The default commands are:

A. ping, traceroute, netstat, and route
B. ping, nslookup, Telnet, and route
C. ping, whois, nslookup, and Telnet
D. ping, traceroute, netstat, and nslookup

Answer: C

NEW QUESTION 44
Which of the following is NOT a VPN routing option available in a star community?

A. To satellites through center only.

B. To center, or through the center to other satellites, to Internet and other VPN targets.
C. To center and to other satellites through center.
D. To center only.

Answer: AD

NEW QUESTION 49
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 54
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 59
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 61
In ClusterXL Load Sharing Multicast Mode:

A. only the primary member received packets sent to the cluster IP address
B. only the secondary member receives packets sent to the cluster IP address
C. packets sent to the cluster IP address are distributed equally between all members of the cluster
D. every member of the cluster received all of the packets sent to the cluster IP address

Answer: D

NEW QUESTION 63
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 67
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 71
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 75
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 77
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 80
Which VPN routing option uses VPN routing for every connection a satellite gateway handles?

A. To satellites through center only
B. To center only
C. To center and to other satellites through center
D. To center, or through the center to other satellites, to Internet and other VPN targets

Answer: D

NEW QUESTION 83
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 88
Which statement is correct about the Sticky Decision Function?

A. It is not supported with either the Performance pack of 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 L2TP traffic

Answer: A

NEW QUESTION 90
What is the port used for SmartConsole to connect to the Security Management Server?

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

Answer: A

NEW QUESTION 92
Which statement is true about ClusterXL?

A. Supports Dynamic Routing (Unicast and Multicast)
B. Supports Dynamic Routing (Unicast Only)
C. Supports Dynamic Routing (Multicast Only)
D. Does not support Dynamic Routing

Answer: A

NEW QUESTION 93
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 94
Which file gives you a list of all security servers in use, including port number?

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

Answer: C

NEW QUESTION 96
To add a file to the Threat Prevention Whitelist, what two items are needed?

A. File name and Gateway
B. Object Name and MD5 signature
C. MD5 signature and Gateway
D. IP address of Management Server and Gateway

Answer: B

NEW QUESTION 101
What is the command to check the status of the SmartEvent Correlation Unit?

A. fw ctl get int cpsead_stat
B. cpstat cpsead
C. fw ctl stat cpsemd
D. cp_conf get_stat cpsemd

Answer: B

NEW QUESTION 105
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 109
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 114
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 116
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 120
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 121
Which process handles connection from SmartConsole R80?

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

Answer: C

NEW QUESTION 126
Full synchronization between cluster members is handled by Firewall Kernel. Which port is used for this?

A. UDP port 265
B. TCP port 265
C. UDP port 256
D. TCP port 256

Answer: D

Explanation:
Synchronization works in two modes:
Full Sync transfers all Security Gateway kernel table information from one cluster member to another. It is handled by the fwd daemon using an encrypted TCP connection on port 256.
Delta Sync transfers changes in the kernel tables between cluster members. Delta sync is handled by the Security Gateway kernel using UDP connections on port 8116.

NEW QUESTION 130
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 133
What is the correct command to observe the Sync traffic in a VRRP environment?

A. fw monitor –e “accept[12:4,b]=224.0.0.18;”
B. fw monitor –e “accept port(6118;”
C. fw monitor –e “accept proto=mcVRRP;”
D. fw monitor –e “accept dst=224.0.0.18;”

Answer: D

NEW QUESTION 138
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 140
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 145
Which file contains the host address to be published, the MAC address that needs to be associated with the IP Address, and the unique IP of the interface that responds to ARP request?

A. /opt/CPshrd-R80/conf/local.arp
B. /var/opt/CPshrd-R80/conf/local.arp
C. $CPDIR/conf/local.arp
D. $FWDIR/conf/local.arp

Answer: D

NEW QUESTION 147
What is the purpose of Priority Delta in VRRP?

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

Answer: C

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

NEW QUESTION 149
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 151
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 155
Fill in the blank: The “fw monitor” tool can be best used to troubleshoot _______.

A. AV issues
B. VPN errors

C. Network issues
D. Authentication issues

Answer: C

NEW QUESTION 158
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 163
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 164
Fill in the blank: Identity Awareness AD-Query is using the Microsoft _______ API to learn users from AD.

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

Answer: A

NEW QUESTION 165
Fill in the blanks. There are________ types of software containers: ________.

A. Three; security management, Security Gateway, and endpoint security
B. Three; Security Gateway, endpoint security, and gateway management
C. Two; security management and endpoint security
D. Two; endpoint security and Security Gateway

Answer: A

NEW QUESTION 166
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 168
What will SmartEvent automatically define as events?

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

Answer: C

NEW QUESTION 172
Fill in the blank: Authentication rules are defined for ________.

A. User groups
B. Users using UserCheck
C. Individual users
D. All users in the database

Answer: A

NEW QUESTION 177
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 181
Which command shows actual allowed connections in state table?

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

Answer: B

NEW QUESTION 185
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 189
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 191
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 196
To optimize Rule Base efficiency, the most hit rules should be where?

A. Removed from the Rule Base.
B. Towards the middle of the Rule Base.
C. Towards the top of the Rule Base.
D. Towards the bottom of the Rule Base.

Answer: C

NEW QUESTION 197
SandBlast has several functional components that work together to ensure that attacks are prevented in real-time. Which the following is NOT part of the SandBlast component?

A. Threat Emulation
B. Mobile Access
C. Mail Transfer Agent
D. Threat Cloud

Answer: C

NEW QUESTION 200
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 202
Fill in the blank: The R80 feature _______ permits blocking specific IP addresses for a specified time period.

A. Block Port Overflow
B. Local Interface Spoofing
C. Suspicious Activity Monitoring
D. Adaptive Threat Prevention

Answer: C

Explanation:
Suspicious Activity Rules Solution
Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).
The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an Install Policy operation.
References:

NEW QUESTION 205
SmartConsole R80 requires the following ports to be open for SmartEvent R80 management:

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

Answer: D

NEW QUESTION 210
After the initial installation on Check Point appliance, you notice that the Management-interface and default gateway are incorrect.
Which commands could you use to set the IP to 192.168.80.200/24 and default gateway to 192.168.80.1.

A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24set static-route default nexthop gateway address 192.168.80.1 onsave config
B. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0add static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0set static-route 0.0.0.0. 0.0.0.0 gw 192.168.80.1 onsave config
D. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24add static-route default nexthop gateway address 192.168.80.1 onsave config

Answer: A

NEW QUESTION 212
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 213
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 214
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 217
Pamela is Cyber Security Engineer working for Global Instance Firm with large scale deployment of Check Point Enterprise Appliances using GAiA/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 221
Which encryption algorithm is the least secured?

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

Answer: C

NEW QUESTION 225
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 226
For best practices, what is the recommended time for automatic unlocking of locked admin accounts?

A. 20 minutes
B. 15 minutes
C. Admin account cannot be unlocked automatically
D. 30 minutes at least

Answer: D

NEW QUESTION 231
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 233
Packet acceleration (SecureXL) identifies connections by several attributes- Which of the attributes is NOT used for identifying connection?

A. Source Address
B. Destination Address
C. TCP Acknowledgment Number
D. Source Port

Answer: C

Explanation:
https //sc1.checkpoint.com/documents/R77/CP R77_Firewall_WebAdmm/92711.htm

NEW QUESTION 234
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 235
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 237
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 242
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 246
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 248
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 253
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 254
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 257
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 259
Which of the following is NOT an alert option?

A. SNMP
B. High alert
C. Mail
D. User defined alert

Answer: B

NEW QUESTION 264
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 266
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 269
When deploying SandBlast, how would a Threat Emulation appliance benefit from the integration of ThreatCloud?

A. ThreatCloud is a database-related application which is located on-premise to preserve privacy of company-related data
B. ThreatCloud is a collaboration platform for all the CheckPoint customers to form a virtual cloud consisting of a combination of all on-premise private cloud environments
C. ThreatCloud is a collaboration platform for Check Point customers to benefit from VMWare ESXi infrastructure which supports the Threat Emulation Appliances as virtual machines in the EMC Cloud
D. ThreatCloud is a collaboration platform for all the Check Point customers to share information about malicious and benign files that all of the customers can benefit from as it makes emulation of known files unnecessary

Answer: D

NEW QUESTION 274
Which of the following links will take you to the SmartView web application?

A. https://<Security Management Server host name>/smartviewweb/
B. https://<Security Management Server IP Address>/smartview/
C. https://<Security Management Server host name>smartviewweb
D. https://<Security Management Server IP Address>/smartview

Answer: B

NEW QUESTION 275

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 276
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 277
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 278
Which command will allow you to see the interface status?

A. cphaprob interface
B. cphaprob –I interface
C. cphaprob –a if
D. cphaprob stat

Answer: C

NEW QUESTION 282
For Management High Availability, which of the following is NOT a valid synchronization status?

A. Collision
B. Down
C. Lagging
D. Never been synchronized

Answer: B

NEW QUESTION 284
Which is NOT a SmartEvent component?

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

Answer: C

NEW QUESTION 288
Which of the following type of authentication on Mobile Access can NOT be used as the first authentication method?

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

Answer: A

NEW QUESTION 290
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 295
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 296
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 298
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 300
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 305
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 309
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 312
Which option, when applied to a rule, allows traffic to VPN gateways in specific VPN communities?

A. All Connections (Clear or Encrypted)
B. Accept all encrypted traffic
C. Specific VPN Communities
D. All Site-to-Site VPN Communities

Answer: B

NEW QUESTION 315
Connections to the Check Point R80 Web API use what protocol?

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

Answer: A

NEW QUESTION 318
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 322
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 324
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 326
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 327
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 330
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 332
What is the default shell of Gaia CLI?

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

Answer: B

NEW QUESTION 334
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 339
Which utility allows you to configure the DHCP service on Gaia from the command line?

A. ifconfig
B. dhcp_ofg
C. sysconfig
D. cpconfig

Answer: C

NEW QUESTION 343
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 346
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 351
Which Check Point daemon monitors the other daemons?

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

Answer: C

NEW QUESTION 355
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 357
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 360
Office mode means that:

A. SecurID client assigns a routable MAC addres
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 addres
F. After the user authenticates for a tunnel, the VPN gateway assigns a routable IP address to the remote client.

Answer: D

NEW QUESTION 364
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 368
What is the Implicit Clean-up Rule?

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

Answer: C

NEW QUESTION 372
Which application should you use to install a contract file?

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

Answer: C

NEW QUESTION 376
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 378
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 382
Security Checkup Summary can be easily conducted within:

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

Answer: B

NEW QUESTION 384
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 389
When an encrypted packet is decrypted, where does this happen?

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

Answer: A

NEW QUESTION 391
What are types of Check Point APIs available currently as part of R80.10 code?

A. Security Gateway API Management API, Threat Prevention API and Identity Awareness Web Services API
B. Management API, Threat Prevention API, Identity Awareness Web Services API and OPSEC SDK API
C. OSE API, OPSEC SDK API, Threat Extraction API and Policy Editor API
D. CPMI API, Management API, Threat Prevention API and Identity Awareness Web Services API

Answer: B

NEW QUESTION 394
How many images are included with Check Point TE appliance in Recommended Mode?

A. 2(OS) images
B. images are chosen by administrator during installation
C. as many as licensed for
D. the most new image

Answer: A

NEW QUESTION 399
Customer's R80 management server needs to be upgraded to R80.10. What is the best upgrade method when the management server is not connected to the Internet?

A. Export R80 configuration, clean install R80.10 and import the configuration
B. CPUSE offline upgrade
C. CPUSE online upgrade
D. SmartUpdate upgrade

Answer: C

NEW QUESTION 402
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-servercommunication

C. Special TCP handshaking extension
D. Supplement DLP data watermark

Answer: B

NEW QUESTION 405
Check Point ClusterXL Active/Active deployment is used when:

A. Only when there is Multicast solution set up.
B. There is Load Sharing solution set up.
C. Only when there is Unicast solution set up.
D. There is High Availability solution set up.

Answer: D

NEW QUESTION 409
Fill in the blank: The IPS policy for pre-R80 gateways is installed during the _______ .

A. Firewall policy install
B. Threat Prevention policy install
C. Anti-bot policy install
D. Access Control policy install

Answer: C

Explanation:
https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents

NEW QUESTION 414
Check Point Management (cpm) is the main management process in that it provides the architecture for a consolidates management console. CPM allows the GUI client and management server to communicate via web services using _______ .

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

Answer: A

NEW QUESTION 419
What is the benefit of “tw monitor” over “tcpdump”?

A. “fw monitor” reveals Layer 2 information, while “tcpdump” acts at Layer 3.
B. “fw monitor” is also available for 64-Bit operating systems.
C. With “fw monitor”, you can see the inspection points, which cannot be seen in “tcpdump”
D. “fw monitor” can be used from the CLI of the Management Server to collect information from multiple gateways.

Answer: C

NEW QUESTION 422
During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:

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

Answer: D

NEW QUESTION 423
Which firewall daemon is responsible for the FW CLI commands?

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

Answer: A

NEW QUESTION 427
......