Checkpoint.Premium.156-115.80.by.VCEplus.100q

156-115.80

Check Point Certified Security Master - R80

Version 1.0

Exam A

QUESTION 1
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
In order to test ClusterXL failovers which command would you use on one of the ClusterXL nodes to initiate a failover?

A. clusterXL_admin down -p

B. cluster XL_admin up -p

C. cphaprob -d TEST -s ok register

D. cphaprob -d TEST -s problem unregister

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm#o97358

QUESTION 3
Which of the following is NOT a valid "fwaccel" parameter?

A. stat

B. stats

C. templates

D. packets

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk41397

QUESTION 4
Which of the following is not one of the relational database domains that stores the management configuration?

A. User Domain

B. System Domain

C. Global Domain

D. Audit Domain

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
What file extension should be used with fw monitor to allow the output file to be imported and read in Wireshark?

A. .cap

B. .exe

C. .tgz

D. .pcap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Where will the usermode core files located?

A. /var/log/dump/usermode
B. /var/suroot
C. $FWDIR/var/log/dump/usermode
D. $CPDIR/var/log/dump/usermode

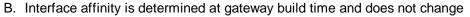**Correct Answer:** A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92764

QUESTION 7
How often will a gateway with Performance Pack running by default automatically review and distribute interface affinity between cores?

A. Every 60 seconds
B. Interface affinity is determined at gateway build time and does not change
C. Every 5 minutes
D. Every 10 seconds

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm

QUESTION 8
Which of the following features is supported in Check Point's implementation of IPv6?

A. Security Servers
B. QoS
C. ClusterXL High Availability

D. SAM

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk39374

QUESTION 9
You verified that Performance Pack is disabled and need to distribute the affinity interfaces. What command would you run to use static affinity to balance the interfaces between the SND cores?

A. cpmq set
B. sim affinity -s
C. fw ctl affinity -a -l -v
D. fw ctl affinity -s

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which command would you use to check CoreXL instances for IPv6 traffic?

A. fwaccel6 stats
B. fwaccel6 stat
C. fw ctl multik stat
D. fw6ctl multik stat

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
What must be done for the "fw monitor" command to capture packets through the firewall kernel?

A. SecureXL must be disabled
B. ClusterXL must be temporarily disabled
C. Firewall policy must be re-installed
D. The output file must be transferred to a machine with WireShark

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

QUESTION 12
Consider a Check Point Security Gateway under high load. What mechanism can be used to confirm that important traffic such as control connections are not dropped?

A. fw debug fgd50 on OPSEC_DEBUG_LEVEL=3
B. fw ctl multik prioq
C. fgate –d load
D. fw ctl debug –m fg all

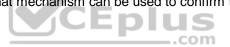**Correct Answer:** A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
What is the default and maximum number of entries in the ARP Cache Table in a Check Point appliance?

A. 1,024 and 4,096
B. 4,096 and 16,384

C. 4,096 and 65,536

D. 1,024 and 16,384

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73181.htm

QUESTION 14
Which kernel debug flag should you use to troubleshoot NAT connections?

A. fw ctl debug + xlate xltrc nat table

B. fw ctl debug + xltrc xlate nat conn

C. fw ctl debug + xlate xltrc nat conn drop

D. fw ctl debug + fwx_alloc nat conn drop

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
You are working with multiple Security Gateways enforcing an extensive number of rules. To simplify security administration, which action would you choose?

A. Eliminate all possible contradictory rules such as the Stealth or Cleanup rules

B. Create a separate Security Policy package for each remote Security Gateway

C. Create network objects that restrict all applicable rules to only certain networks

D. Run separate SmartConsole instances to login and configure each Security Gateway directly

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Which type of SecureXL templates is enabled by default on Security Gateways?

A. Accept
B. Drop
C. NAT
D. VPN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which one of following commands should you run to display HTTPS packet content together with kernel debug?

A. fw ctl get int https_inspection_show_decrypted_data_in_debug=1
   fw ctl get int ssl_inspection_extra_debug=1

B. fw set int https_inspection_get_encrypted_data_in_debug 1
   fw set int https_inspection_show_debug 1

C. fw ctl set int https_inspection_show_decrypted_data_in_debug 1
   fw ctl set int ssl_inspection_extra_debug 1

D. fw ctl set int http_inspection_display_encrypted_data_in_debug=1
   fw ctl set int http_inspection_extra_debug=1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You issued the command "set ipv6-state on" in order to enable IPv6 protocol on a Security Gateway. The command was executed successfully. After reboot you notice that IPv6 protocol is not enabled. What do you do to permanently enable IPv6 protocol?

A. Issue "set ipv6-state on" again; Save configuration and reboot

B. You need to modify Gateway Properties in SmartConsole and install policy in order to enable IPv6

C. You need to set "ipv6_state" parameter in $FWDIR/boot/modules/fwkern.conf and reboot

D. You need to install a valid license to use IPv6 protocol

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Where does the translation occur with Hide NAT?

A. The destination translation occurs at the client side

B. The source translation occurs at the server side

C. The source translation occurs at the client side

D. The destination translation occurs at the server side

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Fill in the blank. The tool _____ generates a R80 Security Gateway configuration report.

A. `infoCP`

B. `infoview`

C. `cpinfo`

D. `fw cpinfo`

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 21
Which is the correct "fw monitor" syntax for creating a capture file for loading it into WireShark?

A. fw monitor –e "accept <FILTER EXPRESSION>; ">> Output.cap
B. This cannot be accomplished as it is not supported with R80.10
C. fw monitor –e "accept <FILTER EXPRESSION>;" –file Output.cap
D. fw monitor –e "accept <FILTER EXPRESSION>;" –o Output.cap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
How many layers are incorporated in IPS detection and what are they called?

A. 4 layers – Passive Streaming Library (PSL), Protocol Parsers, Context Management, Protections
B. 3 layers – Active Streaming Library (ASL), CMI, Protections
C. 4 layers – Active Streaming Library (ASL), Protocol Parsers, Context Management, Protections
D. 3 layers – Protocol Parsers, CMI, Protections

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
What is the command to check the current status of hyper-threading?

A. fw ctl get int cphwd_hyper_status
B. fw ctl multik stat
C. cat/proc/hyperstats
D. cat/proc/smt_status

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93000#To%20check%20SMT%20current%20status

QUESTION 24
What occurs when Bypass Under Load activated?

A. Packets are forwarded to the destination without checking the packets against the firewall rule base
B. Packets are forwarded to the destination without performing IPS analysis
C. To still ensure a minimum level of data integrity, the system revert to the use of MD5 instead of SHA-1, since former produces an output smaller than the latter
D. The amount of the state table entries is decreased according to the LRU (least recently used) algorithm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IPS_AdminGuide/12750.htm

QUESTION 25
Having a look at the output of the "fwaccel conns" command, the F flag is the indicator for a packet _____.

A. getting the routing information according to the Forwarding Information Base (FIB)
B. being processed by the firewall kernel module
C. going through the slow path
D. being forced of using the accelerated path

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Of how many packets consists Main Mode in Phase 1?

A. Three packets
B. Four packets
C. Six packets
D. it depends on the encryption algorithm used. 3DES has three times more packets than DES encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
What does the command "vpn shell tunnels delete all ike" do?

A. Delete only outbound_SPI tables
B. Deletes all IKE and IPSEC SA's
C. Deletes all IKE configuration on the Gateway
D. Deletes all IKE SA's

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
When enabling hyper-threading on a Security Gateway, the administrator needs to make sure there is enough _____ to support additional CoreXL Firewall instances.

A. drive space

B. cpu's

C. available cache

D. available memory

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93000

QUESTION 29
You run "cat/proc/smt_status" on your security gateway and the output shows 'Soft Disable'. How is your system configured in reference to hyper-threading?

A. Hyper-threading is disabled in BIOS and cpconfig

B. Hyper-threading is enabled in BIOS but disabled in cpconfig

C. Hyper-threading is disabled in BIOS but enabled in cpconfig

D. Your system does not support Hyper-threading

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk93000

QUESTION 30
Which command is used to enable IPv6 on Security Gateway?

A. set ipv6-state on

B. add ipv6 interface on

C. set ipv6-enable on

D. set ipv6-state enabled

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:

QUESTION 31
What is the correct command to turn off an IKE debug?

A. vpn debug ikeoff
B. fw ctl debug ikeoff
C. vpn debug ikeoff 0
D. fw ctl vpn debug ikeoff

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.checkpoint.com/docs/DOC-3023-vpn-troubleshooting-commands

QUESTION 32
What process(es) should be checked if there is high I/O and you suspect it may be related to the Antivirus Software Blade?

A. avsp
B. dlpu and rad processes
C. cpta
D. cpm and fwm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Which of the following is NOT a special consideration while running fw monitor on production firewall?

A. While executing fw monitor, you need to specify an expression so that it captures the required traffic instead of all traffic

B. While running fw monitor on a busy firewall, the –ci <count> and –co <count> switches can be used to limit the number of packets captured

C. While running fw monitor, it resets all the debug flags

D. During a fw monitor, the firewall will have to process more packets because SecureXL acceleration should be disabled

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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 an authorized IP address

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following inputs is suitable for debugging HTTPS inspection issues?

A. vpn debug cptls on

B. fw ctl debug –m fw + conn drop cptls

C. fw diag debug tls enable

D. fw debug tls on TDERROR_ALL_ALL=5

Correct Answer: B
Section: (none)
Explanation

QUESTION 36
Which of the connections cannot be accelerated with SecureXL?

A. Every NAT'ed connection

B. Every encrypted connection, such as HTTPS or SSH connections

C. Every connection destined to the Security Gateways

D. Every connection through a rule using a time object

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following ports are used for SIC?

A. 18355 and 18356

B. 18210 and 18211

C. 257 and 258

D. 18192 and 18193

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://digitalcrunch.com/check-point-firewall/list-of-check-point-ports/

QUESTION 38
Joey's implementing a new R80.10 firewall cluster into the network. During the implementation he notices that the cluster object is in error state in SmartConsole.
He tries to figure out the cause of the problem and runs a ClusterXL kernel debug with command: 'fw ctl debug –m cluster + stat pnote conf ccp'
ClusterXL kernel debug shows him following info: fwha_set_new_local_state: Old version HA machines exist around so prevent state change to READY.
How can he solve the problem?

A. cphaconf cluster_id set <NEW_CLUSTER_ID_VALUE>

B. cphaprob mmagic

C. Connect with GuiDBedit Tool to Security Management Server. Go to Table – Network Objects – network_objects. Select the relevant R80.10 Cluster object. Go to Search menu – Find – paste mac_magic. Right-click on the mac_magic the object – select Edit… and change the value to 254. Save changes and install policy.

D. Connect with GuiDBedit Tool to Security Management Server. Go to Table – Network Objects – network_objects. Select the relevant R80.10 Cluster object. Go to Search menu – Find – paste cluster_magic. Right-click on the cluster_magic the object – select Edit… and change the value between 1 and 253. Save changes and install policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk25977

QUESTION 39
Which file would you need to make sure you collect when debugging a VPN that fails to establish that is configured to use IKEv2?

A. $FWDIR/log/ike2.elg

B. $FWDIR/log/vpnd.xml.v2

C. $FWDIR/log/ikev2.xml

D. $CPDIR/log/ike.elg

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=skI4326

QUESTION 40
What is the name of the table that an administrator would review to investigate a port exhaustion error when using Hide NAT?

A. dyn_nat_table

B. connection

C. nat_dyn_table

D. fwx_alloc

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk32224

QUESTION 41
After determining that the IPS Blade is causing high resource utilization in the gateway, which would be an appropriate strategy to improve IPS performance?

A. Enabling CoreXL
B. Enable Bypass mode
C. Disabling SecureXL
D. Enabling SecureXL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which process is responsible for the generation of certificates?

A. cpm
B. cpca
C. dbsync
D. fwm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638#Security%20Management%

20Software%20Blades%20and%20Features%20-%20SmartLog

QUESTION 43
Which one of the following does not belong to an initial status of a critical device?

A. restart
B. problem
C. init
D. ok

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

QUESTION 44
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
What is enabled by the command "vpn debug mon"?

A. statistics monitoring for vpn encrypted packets
B. vpn daemon monitor mode
C. ike monitor
D. vpn debug mode

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Fill in the blank: The R80 utility `fw monitor` is used to troubleshoot _____.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which daemon would you debug if you have issues acquiring identities via identity sharing and identities with other gateways?

A. pdpd
B. wstlsd
C. iad
D. pepd
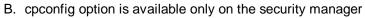
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/66477.htm

QUESTION 49
What is the difference between disabling SecureXL by running "fwaccel off" and disabling it via cpconfig?

A. Disabling SecureXL in cpconfig survives reboot
B. cpconfig option is available only on the security manager
C. There is no difference. These are two different ways of accomplishing the same task
D. "fwaccel off" will survive the reboot but cpconfig will not

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk41397

QUESTION 50
What is the role of FWM process in Check Point R80.10 Security Management architecture?

A. It is called by CPM process to perform verification and conversion of the database
B. FWM is used to transfer CPsets from management to the gateway
C. FWM prepares and loads commit functions to execute the policy
D. Policy installation command initiated from SmartConsole is sent to FWM

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101226

QUESTION 51
Which IPS command debug tool can you use for troubleshooting IPS traffic?

A. ips debug traffic –o IPSdebug
B. ips debug –f /var/log/IPSdebug.txt
C. debug ips enable –o IPSdebug
D. ips debug –o IPSdebug

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/84627.htm#o84632

QUESTION 52
Which of the following would NOT be a flag when debugging a unified policy?

A. rulebase
B. clob
C. connection
D. tls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120964

QUESTION 53

What is the shorthand reference for a classification object?

A. CLOB
B. class.obj
C. classobj
D. COBJ

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120964

QUESTION 54
To manually configure the number of CoreXL instances running on a gateway, what steps must be taken?

A. cpconfig – Configure Check Point CoreXL – Choose the number of firewall instances –exit - Reboot
B. cpstop – cpconfig – Configure Check Point CoreXL – Choose the number of firewall instances –exit - cpstart
C. Uninstall license – cpconfig – Configure Check Point CoreXL – Choose the number of firewall instances – Install license – Exit
D. cpconfig – Configure Check Point CoreXL – Choose the number of firewall instances -exit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/6731.htm

QUESTION 55
Where do Protocol parsers register themselves for IPS?

A. Passive Streaming Library
B. Other handlers register to Protocol parser
C. Protections database
D. Context Management Infrastructure

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.nwtechusa.com/pdf/checkpoint_blade_ips.pdf

QUESTION 56
Which command is used to write a kernel debug to a file?

A. fw ctl debug –T –f > debug.txt
B. fw ctl kdebug –T –l > debug.txt
C. fw ctl debug –S –t > debug.txt
D. fw ctl kdebug –T –f > debug.txt

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://itsecworks.com/2011/08/09/checkpoint-firewall-debugging-basics/

QUESTION 57
Which database domain stores URL filtering updates?

A. Threat Prevention Domain
B. Application Control domain
C. IPS Domain
D. Check Point Data Domain

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
John works for ABC Corporation. They have enabled CoreXL on their firewall. John would like to identify the cores on which the SND runs and the cores on which the firewall instance is running. Which command should John run to view the CPU role allocation?

A. fw ctl affinity –v
B. fwaccel stat –l
C. fw ctl affinity –l
D. fw ctl cores

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
How can you force a manual failover?

A. cphaconf set_force_failover 1
B. kill -15 vpnd
C. clusterXL_admin down
D. fw ctl set int fwha_failover 1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://fwknowledge.wordpress.com/2013/04/04/manual-failover-of-the-fw-cluster/

QUESTION 60
What ClusterXL mechanism is used to verify that the interfaces of other cluster members are UP and communicates the status of cluster members?

A. PING
B. CCP
C. PPP
D. HELLO

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:

QUESTION 61
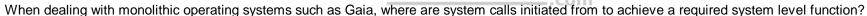Which of the following commands can be used to see the list of processes monitored by the Watch Dog process?

A. cpwd_admin list
B. ps –ef | grep watchd
C. cpstat fw –f watchdog
D. fw ctl get str watchdog

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.checkpoint.com/thread/8054-cpwdadmin-list-overview-sms

QUESTION 62
When dealing with monolithic operating systems such as Gaia, where are system calls initiated from to achieve a required system level function?

A. Slow Path
B. Medium Path
C. Kernel Mode
D. User Mode

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which Check Point utility should be used to assist in analyzing the output of vpn and ike debug?

A. cpview
B. cpinfo
C. ikeview
D. vpnview

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/12467.htm

QUESTION 64
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
What is the default setting and minimum value of the Sync tick timer?

A. 500ms
B. 1000ms
C. 100ms
D. 1500ms

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

QUESTION 66
What effect would change the parameter of fwha_timer_cpha_res to 5 have on a cluster?

A. Change the cluster interface active check to 5 milliseconds

B. Change the cphad to send test packets every 5 milliseconds

C. Change the sync network timeout to 5 seconds

D. Change the failover delay timeout to 500 milliseconds

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

QUESTION 67
Your customer is experiencing problems connecting to the Security Management Server via SmartConsole. You suggest testing the connection to the SMS with GuiBedit from the client machine. This connection was successful. Now you suggest enabling debug to investigate possible issues with connections to SMS via SmartConsole. Which process does the customer need to debug on the SMS?

A. cpd

B. fwd

C. cpm

D. fwm

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

QUESTION 68
If cluster members are geographically separated and the time to detect a failover needs to be longer, what timer needs to be adjusted?

A. fwha_timer_cpha_res
B. fwha_timer_dist_res
C. fwha_geosync_timer
D. fwha_timer_sync_res

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

QUESTION 69
Which command should be used to insert fw monitor before secxl_sync module?

A. fw monitor –pi –secxl_sync –o capture.cap
B. fw monitor –pl –secxl_sync –o capture.cap
C. fw monitor –pO –secxl_sync –o capture.cap
D. fw monitor –e "accept –pi –secxl_sync;" –o capture.cap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
What is the difference between Client-Side and Server-Side NAT?

A. The translation occurs at the kernel nearest the server for client-side NAT, but for server-side NAT, the translation occurs at the kernel nearest the client
B. The translation occurs at the kernel nearest the server in both cases. So, there is no difference at all
C. The translation occurs at the kernel nearest the client for client-side NAT, but for server-side NAT, the translation occurs at the kernel nearest the server
D. The translation occurs at the kernel nearest the client in both cases. So, there is no difference at all

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
If certain services should not use the Cluster Object IP Address, but requires the use of the individual Cluster Member IPs, what steps would be required for configuration?

A. Create Manual NAT rules in the Security Policy
B. The configuration is not possible
C. Edit the table.def file on the Management Server
D. Edit the fwkern.conf on each Cluster Member

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
The maximum number of critical devices or pnotes on a cluster member is what?

A. 8
B. 24
C. 32
D. 16

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

QUESTION 73
What does CMI stand for in relation to the Access Control Policy?

A. Content Matching Infrastructure
B. Content Management Interface
C. Context Management Infrastructure
D. Context Manipulation Interface

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.checkpoint.com/thread/6199-classifying-traffic-to-match-unified-policy-column-objects

QUESTION 74
A Firewall administrator is attempting to push a policy to a new Security Gateway for a remote office but the installation fails. The Management Server IP is 10.1.1.101. Initial troubleshooting shows that policy is successfully transferred to the Gateway. What command would you use to attempt to identify the cause of the issue?

A. fw ctl debug –T –f > /var/log/p_debug.txt
B. cp_merge export_policy –s 10.1.1.101 –n Standard $var/log/
C. fw ctl debug –m 10.1.1.101
D. fw fetchlocal –d $FWDIR/state/_tmp/FW1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Where will the command, "fw monitor -pi -vpn", be inserted into the ctl chain?

A. Before the Fw VM inbound
B. Before the vpn module
C. After the Fw VM outbound
D. After the vpn module

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which "fwm" command syntax will instruct the gateway to load its most recent policy?

A. fwm fetch localhost
B. fwm –d fetchlocal
C. fwm load <policy_name> -m <management_IP>
D. None, as "fwm" can only be executed on management servers

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following is correct in a Threat Prevention policy?

A. Threat Prevention inspects traffic to all objects specified in the Protected Scope
B. Threat Prevention inspects traffic to and/or from all objects specified in the Protected Scope
C. Threat Prevention is applied based on the profile. Protection Scope does not have any relevance
D. Threat Prevention inspects traffic from all objects specified in the protected Scope

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_ThreatPrevention_AdminGuide/html_frameset.htm?
topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_ThreatPrevention_AdminGuide/136933

QUESTION 78
Which Check Point daemon, if it stops responding or goes down, results in connections from the SmartConsole to the Management Server failing?

A. SMSD
B. CPTA
C. CPM
D. FWD

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
How can you ensure that a particular service does not use the cluster IP address?

A. Add the corresponding service port and IP protocol number into the "no_hide_services_ports" section of the table.def file
B. Add the corresponding service port and IP protocol number into the "hide_services_ports" section of the table.def file
C. Add the corresponding service port and IP protocol number into the "no_hide_services_ports" section of the user.def file
D. Add the corresponding service port and IP protocol number into the "hide_services_ports" section of the user.def file

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required?

A. RAD Kernel Space
B. URLF Kernel Client
C. URLF Online Service
D. RAD User Space

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference: https://community.checkpoint.com/thread/9034-url-filtering-using-dns

QUESTION 81
Which templates for SecureXL are not enabled by default?

A. All templates are disabled by default
B. Accept and NMR
C. Drop and NAT
D. All templates are enabled by default

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk71200

QUESTION 82
While using IPS, the network performance is being impacted on a load sharing cluster with asymmetric routes. What is most likely causing the degradation?

A. A failure in the sync network protocol
B. A static NAT has been configured and an IPS protection requires the connection be handled on the same cluster member
C. CoreXL has been disabled
D. SecureXL has been disabled

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Which kernel table stores information about NAT connections?

A. connections
B. tab_nat_conn
C. xlate
D. fwx_alloc

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk32224

QUESTION 84
How can you print the session UUID and the UUID of a connection together in fw monitor?

A. The switches –s and –u are mutually exclusive and cannot be printed together
B. fw –s monitor –u –e "accept <FILTER EXPRESSION>;"
C. fw monitor –uids –e "accept <FILTER EXPRESSION>;"
D. fw monitor –s –u –e "accept <FILLTER EXPRESSION>;"

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

QUESTION 85
The pepd and pdpd daemons are used by which Software blade?

A. Identity Awareness
B. DLP
C. URL Filtering
D. Application Control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
For organizations with existing IPv4 networks who wish to move to IPv6, which of the following is a Transition Mechanism that can be used?

A. ipv4 to ipv6 Triple Stack
B. Hex to Dec translation
C. 6 in 4 Tunneling
D. NAT-T to NAT6sec

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which command query will search the database for instances of the following FW-Corporate object:

A. select name from dleobjectderef_data where name = 'FW-Corporate';
B. select data from dleobjectderef_data where name = 'FW-Corporate';
C. select object 'FW-Corporate' from dleobjectderef_data;
D. select name from dleobjectderef_table where name = 'FW-Corporate';

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
When running a debug with fw monitor, which parameter will create a more verbose output?

A. -l

B. -i

C. -D

D. -d

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30583

QUESTION 89
Which daemon is responsible for anti-spam?

A. cpmd

B. ctasd

C. ctmd

D. cpemd

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

QUESTION 90
IPS detection incorporates 4 layers. Which of the following is NOT a layer in IPS detection?

A. Context Management

B. Protocol Parsers

C. Protections

D. Detections

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91

When troubleshooting acceleration issues on a Security Gateway, you notice that the fw_worker_x process is consuming about 100% processing power. What can be done to stop this from happening?

A. Assign more CPU cores to the system
B. Use fwaccel stop/start release process
C. Edit the registry file to increase virtual memory
D. Remove the memory file in /proc/ and recreate it

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92

Which of the following is NOT a feature of ClusterXL?

A. Transparent upgrades
B. Zero downtime for mission-critical environments with State Synchronization
C. Enhanced throughput in all ClusterXL modes (2 gateway cluster compared with 1 gateway)
D. Transparent failover in case of device failures

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

QUESTION 93

Static NAT has been configured and NAT rules were created automatically. The global properties option "Translate destination on client side" is not checked. Clients are complaining that they are not able to connect to one of your web servers using its public address. How would you solve the problem without changing the global properties and reinstalling the security policy?

A. On the security gateway, add a static route for the web server's public ip address
B. Rebooting the security gateway will resolve the problem
C. You will have the global properties and reinstall the security policy
D. Configure manual NAT

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Consider an IKE debug file that has been generated when debugging an issue with site to site VPN. What is the purpose of a NONCE?

A. Randomly generated part of key generation
B. Vendor ID and Remote Gateway ID
C. Protocol 50 and 51 representations
D. Fixed hex value of Phase 2 keys with PFS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96

In order to review the IPS statistics to determine if adjustments can be made to improve performance, which command would you use to get the appropriate information?

A. fw monitor –e "accept IPS_stats;" >> ips_statistics.xml
B. fw ctl debug –m ips debug_compilation
C. fw ctl set int enable_ips_debug_output 1
D. $FWDIR/scripts/get_ips_statistics.sh 10.1.1.1 60

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97

The CPM process uses what ports?

A. 19009 and 18120
B. 18265 and 257
C. 19009 and 9009
D. 18265 and 9009

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R80/CP_R80_MultiDomainSecurity/html_frameset.htm?topic=documents/R80/CP_R80_MultiDomainSecurity/15420

QUESTION 98

You need to investigate issues with policy installation on the Security Gateway side. Which process will you debug and how?

A. cpd; cpd_admin debug on TDERROR_ALL_ALL=5

B. cpd; fw ctl debug on –m cpd

C. fwm; fw debug fwm on TDERROR_ALL_ALL=5

D. fwd; fw debug fwd on TDERROR_ALL_ALL=5

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/11844/FILE/How-To-Troubleshoot-Policy-Installation-Issues.pdf

QUESTION 99
What is the proper syntax to enter the "central database" that contains all objects within the Postgres database?

A. psql_client cpm postgres

B. psql_client checkpoint postgres

C. psql_client central_database postgres

D. In clish: show postgres main

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In a high traffic network, which feature allows for more than one traffic path on an interface so that more than one CPU can be used for acceleration?

A. interface bonding

B. vlan

C. asic

D. multi queue

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/93689.htm