156-115.80.52q

Number: 156-115.80
Passing Score: 800
Time Limit: 120 min

156-115.80

Check Point Certified Security Master - R80

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
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 3

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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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

Explanation/Reference:
Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

QUESTION 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29

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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
Which templates for SecureXL are not enabled by default?

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

https://vceplus.com/

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 39
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 40
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 41

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 42
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 43
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 44
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 45
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 46
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 47
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 48
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 49
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 50
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 51

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 52
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: