156-115.80.exam.44q

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

156-115.80

Check Point Certified Security Master - R80

Exam A

QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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 18
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 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
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41

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 42
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 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