156-915.80$^{Q\&As}$

Check Point Certified Security Expert Update - R80.10

Pass CheckPoint 156-915.80 Exam with 100% Guarantee

QUESTION 1

What CLI command will reset the IPS pattern matcher statistics?

A. ips reset pmstat

B. ips pstats reset

C. ips pmstats refresh

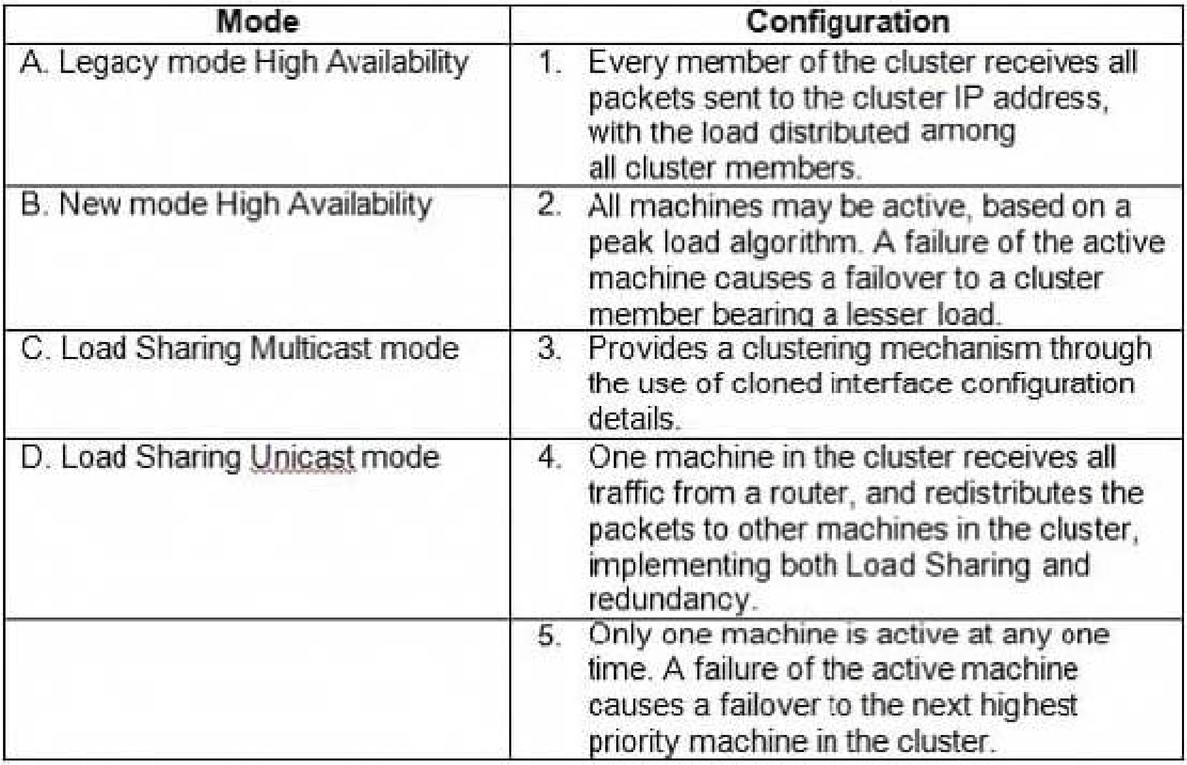
D. ips pmstats reset

Correct Answer: D

ips pmstats reset Description - Resets the data that is collected to calculate the pmstat statistics. Usage - ips pmstats reset Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/84627.htm#o84635

QUESTION 2

Match the ClusterXL modes with their configurations. Exhibit:



Mode	Configuration
A. Legacy mode High Availability	1. Every member of the cluster receives all packets sent to the cluster IP address, with the load distributed among all cluster members.
B. New mode High Availability	2. All machines may be active, based on a peak load algorithm. A failure of the active machine causes a failover to a cluster member bearing a lesser load.
C. Load Sharing Multicast mode	3. Provides a clustering mechanism through the use of cloned interface configuration details.
D. Load Sharing Unicast mode	4. One machine in the cluster receives all traffic from a router, and redistributes the packets to other machines in the cluster, implementing both Load Sharing and redundancy.
	5. Only one machine is active at any one time. A failure of the active machine causes a failover to the next highest priority machine in the cluster.

A. A-2, B-3, C-4, D-1

B. A-2, B-3, C-1, D-5

C. A-3, B-5, C-1, D-4

D. A-5, B-2, C-4, D-1

Correct Answer: C

QUESTION 3

What is true about VRRP implementations?

A. VRRP membership is enabled in cpconfig

B. VRRP can be used together with ClusterXL, but with degraded performance

C. You cannot have a standalone deployment

D. You cannot have different VRIDs in the same physical network

Correct Answer: C

Reference: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_AdminWebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_AdminWebAdminGuide/87911

QUESTION 4

In which case is a Sticky Decision Function relevant?

A. Load Sharing ?Multicast

B. Load Balancing ?Forward

C. High Availability

D. Load Sharing ?Unicast

Correct Answer: C

QUESTION 5

Which command would provide the most comprehensive diagnostic information to Check Point Technical Support?

A. fw cpinfo

B. cpinfo -o date.cpinfo.txt

C. diag

D. cpstat - date.cpstat.txt

Correct Answer: B

QUESTION 6

What is the purpose of the pre-defined exclusions included with SmartEvent R80?

A. To allow SmartEvent R80 to function properly with all other R71 devices.

B. To avoid incorrect event generation by the default IPS event definition; a scenario that may occur in deployments that include Security Gateways of versions prior to R71.

C. As a base for starting and building exclusions.

D. To give samples of how to write your own exclusion.

Correct Answer: B

QUESTION 7

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

A. fwd via cpm

B. fwm via fwd

C. cpm via cpd

D. fwd via cpd

Correct Answer: AB

QUESTION 8

How are cached usernames and passwords cleared from the memory of a R80 Security Gateway?

A. By using the Clear User Cache button in SmartDashboard.

B. Usernames and passwords only clear from memory after they time out.

C. By retrieving LDAP user information using the command fw fetchldap.

D. By installing a Security Policy.

Correct Answer: D

QUESTION 9

What is the command to show SecureXL status?

A. fwaccel status

B. fwaccel stats -m

C. fwaccel -s

D. fwaccel stat

Correct Answer: D

To check overall SecureXL status: [Expert@HostName]# fwaccel stat Reference: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=andsolutionid=sk41397

QUESTION 10

What\\'s true about Troubleshooting option in the IPS profile properties?

A. Temporarily change the active protection profile to "Default_Protection"

B. Temporarily set all protections to track (log) in SmartView Tracker

C. Temporarily will disable IPS kernel engine

D. Temporarily set all active protections to Detect

Correct Answer: B

Reference: https://sc1.checkpoint.com/documents/R76/CP_R76_IPS_AdminGuide/52512.htm

QUESTION 11

You are troubleshooting a HTTP connection problem. You\\'ve started fw monitor -o http.pcap. When you open http.pcap with Wireshark there is only one line. What is the most likely reason?

A. fw monitor was restricted to the wrong interface.

B. Like SmartView Tracker only the first packet of a connection will be captured by fw monitor.

C. By default only SYN pakets are captured.

D. Acceleration was turned on and therefore fw monitor sees only SYN.

Correct Answer: D

QUESTION 12

Which operating systems are supported by a Check Point Security Gateway on an open server? Select MOST complete list.

A. Sun Solaris, Red Hat Enterprise Linux, Check Point SecurePlatform, IPSO, Microsoft Windows

B. Check Point GAiA and SecurePlatform, and Microsoft Windows

C. Check Point GAiA, Microsoft Windows, Red Hat Enterprise Linux, Sun Solaris, IPSO

D. Check Point GAiA and SecurePlatform, IPSO, Sun Solaris, Microsoft Windows

Correct Answer: B

QUESTION 13

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

A. Threat Emulation never delivers a file and takes more than 3minutes to complete

B. Threat Extraction always delivers a file and takes less than a second to complete

C. Threat Emulation never delivers a file that takes less than a second to complete

D. Threat Extraction never delivers a file and takes more than 3 minutes to complete

Correct Answer: B

QUESTION 14

To fully enable Dynamic Dispatcher on a Security Gateway:

A. run "fw ctl multik dynamic_dispatching on" and then reboot

B. Using cpconfig, update the Dynamic Dispatcher value to "full" under the CoreXl menu

C. Edit /proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot

D. run fw ctl multik set_mode 1 in Expert mode and then reboot

Correct Answer: A

QUESTION 15

SmartEvent has several components that function together to track security threats. What is the function of the Correlation Unit as a component of this architecture?

A. Analyzes this log entry as it arrives at the log server according to the Event Policy. When a threat pattern is identified, an event is forwarded to the SmartEvent Server.

B. Correlates all the identified threats with the consolidation policy.

C. Collects syslog data from third party devices and saves them to the database.

D. Connects with the SmartEvent Client when generating threat reports.

Correct Answer: A