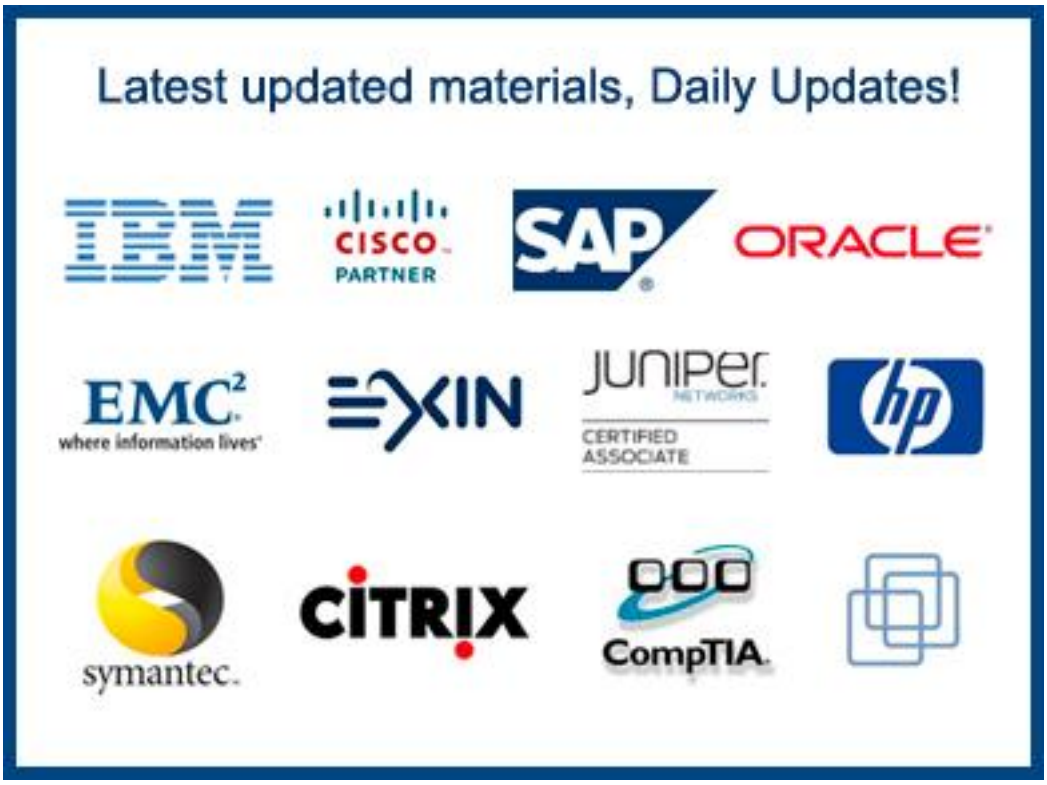
BraindumpStudy

BraindumpStudy
Leader of IT Certifications Study



http://www.braindumpstudy.com

BraindumpStudy Exam Dumps, High Pass Rate!

Exam : **156-915.80**

Title : Check Point Certified Security Expert Update - R80

Vendor : CheckPoint

Version : DEMO

NO.1 Which statement is true regarding redundancy?
A. System Administrator know when their cluster has failed over and can also see why it failed over by using the cphaprob f it command.
B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
C. Both Cluster XL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.
D. Machines in a Cluster XL High Availability configuration must be synchronized.
Answer: C

NO.2 Choose the ClusterXL process that is defined by default as a critical device?
A. fwd
B. cpp
C. fwm
D. assld
Answer: A

NO.3 Use the table to match the BEST Management High Availability synchronication-status descriptions for your Security Management Server (SMS).
Exhibit:

Status	Description
A. Never synchronized	1. The active SMS has changed but the standby SMS has not been synchronized.
B. Lagging	2. The standby SMS changed before the active SMS.
C. Advanced	3. The secondary server needs to be manually synchronized with the primary.
D. Collision	4. The active and standby SMS's have both been changed without a successful synchronization.
	5. The standby SMS has changed more recently than the active SMS.

A. A-3, B-5, C-2, D-4
B. A-3, B-1, C-5, D-4
C. A-5, B-3, C-1, D-2
D. A-3, B-1, C-4, D-2
Answer: B

NO.4 How long may verification of one file take for Sandblast Threat Emulation?
A. within seconds cleaned file will be provided
B. up to 5 minutes
C. up to 3 minutes
D. up to 1 minutes
Answer: A

NO.5 What is correct statement about Security Gateway and Security Management Server failover in Check Point R80.X in terms of Check Point Redundancy driven solutions?
A. Security Gateway failover is an automatic procedure but Security Management Server failover is a manual procedure.
B. Security Gateway failover as well as Security Management Server failover is an automatic procedure.
C. Security Gateway failover is a manual procedure but Security Management Server failover is an automatic procedure.
D. Security Gateway failover as well as Security Management Server failover is a manual procedure
Answer: A

NO.6 What is the mechanism behind Threat Extraction?
A. This is a new mechanism which extracts malicious files from a document to use it as a counter-attack against its sender
B. This is a new mechanism to identify the IP address of the sender of malicious codes and to put it into the SAM database (Suspicious Activity Monitoring).
C. This is a new mechanism which is able to collect malicious files out of any kind of file types to destroy it prior to sending it to the intended recipient
D. Any active contents of a document, such as JavaScripts, macros and links will be removed from the document and forwarded to the intended recipient, which makes this solution very fast.
Answer: D

NO.7 What happen when IPS profile is set in Detect-Only Mode for troubleshooting?
A. Automatically uploads debugging logs to Check Point Support Center
B. It will generate Geo-Protection traffic
C. It will not block malicious traffic
D. Bypass licenses requirement for Geo-Protection control
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.
Answer: C

NO.8 Select the command set best used to verify proper failover function of a new ClusterXL configuration.
A. cphaprob -d failDevice -s problem -t 0 register / cphaprob -d failDevice unregister
B. cpstop/cpstart
C. reboot
D. clusterXL_admin down / clusterXL_admin up
Answer: D

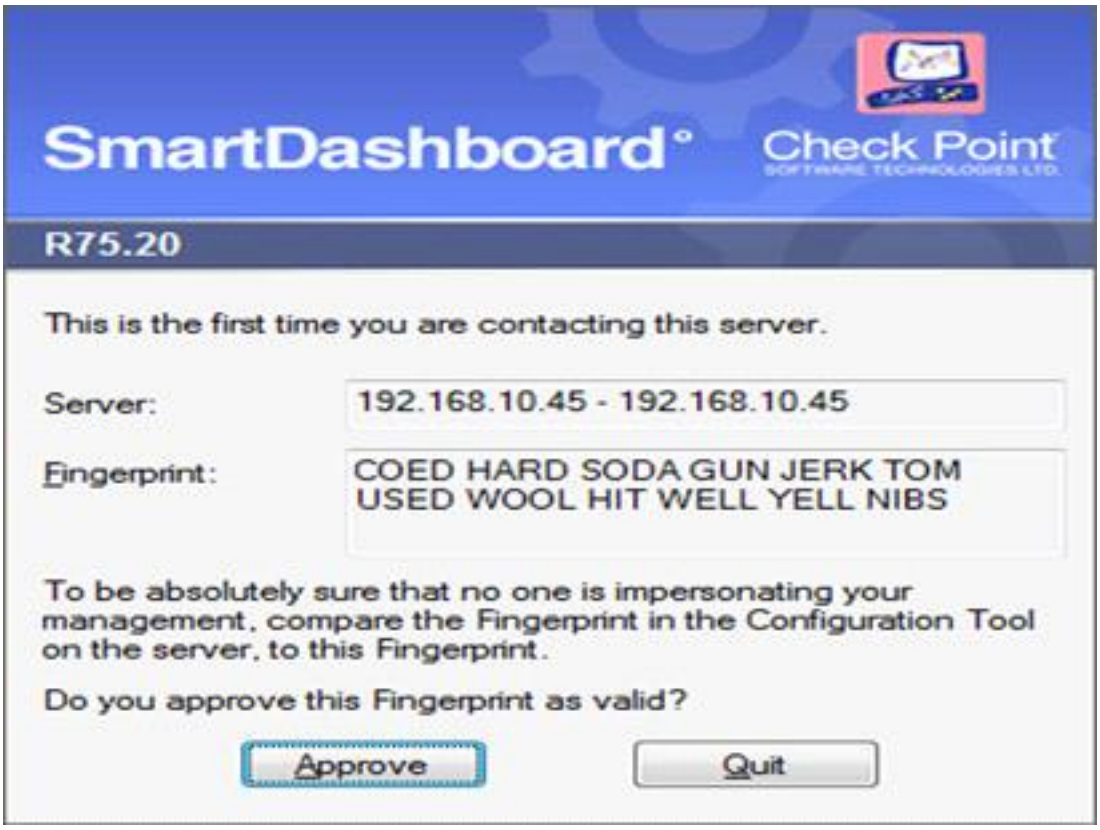
NO.9 You are asked to check the status of several user-mode processes on the management server and gateway.
Which of the following processes can only be seen on a Management Server?

A. fwm
B. fwd
C. cpd
D. cpwd
Answer: A

NO.10 Your main internal network 10.10.10.0/24 allows all traffic to the Internet using Hide NAT. You also have a small network 10.10.20.0/24 behind the internal router. You want to configure the kernel to translate the source address only when network 10.10.20.0 tries to access the Internet for HTTP, SMTP, and FTP services. Which of the following configurations will allow this network to access the Internet?
A. Configure Automatic Static NAT on network 10.10.20.0/24.
B. Configure three Manual Static NAT rules for network 10.10.20.0/24, one for each service.
C. Configure one Manual Hide NAT rule for HTTP, FTP, and SMTP services for network 10.10.20.0/24.
D. Configure Automatic Hide NAT on network 10.10.20.0/24 and then edit the Service column in the NAT Rule Base on the automatic rule.
Answer: C

NO.11 Which of the following is NOT an internal/native Check Point command?
A. fw ct1 debug
B. cphaprob
C. tcpdump
D. fwaccel on
Answer: C

NO.12 How could you compare the Fingerprint shown to the Fingerprint on the server?
Exhibit:



A. Run cpconfig, select the Certificate's Fingerprint option and view the fingerprint
B. Run cpconfig, select the Certificate Authority option and view the fingerprint
C. Run sysconfig, select the Server Fingerprint option and view the fingerprint
D. Run cpconfig, select the GUI Clients option and view the fingerprint
Answer: A

NO.13 Which command collects diagnostic data for analyzing customer setup remotely?
A. cpview
B. sysinfo
C. cpinfo
D. migrate export
Answer: C
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.

NO.14 Which statements below are CORRECT regarding Threat Prevention profiles in SmartConsole?
A. You can assign multiple profiles per gateway and a profile can be assigned to one or more rules.
B. You can assign only one profile pre gateway and a profile can be assigned to one or more rules.
C. You can assign multiple profiles per gateway and a profile can be assigned to one rule only.
D. You can assign only one profile per gateway and a profile can be assigned to one rule Only.

Answer: A

NO.15 How many interfaces can you configure to use the Multi-Queue feature?
A. 4 interfaces
B. 3 interfaces
C. 5 interfaces
D. 10 interfaces
Answer: C
References:
https://community.checkpoint.com/t5/Enterprise-Appliances-and-Gaia/R80-x-Performance-Tuning-Tip-Multi-Queue/td-p/41608

NO.16 When configuring numbered VPN Tunnel Interfaces (VTIs) in a clustered environment, what issues need to be considered?
1) Each member must have a unique source IP address.
2) Every interface on each member requires a unique IP address.
3) All VTI's going to the same remote peer must have the same name.
4) Cluster IP addresses are required.
A. 2 and 3
B. 1, 2, 3 and 4
C. 1, 2, and 4
D. 1, 3, and 4
Answer: B

NO.17 Jack needs to configure CoreXL on his Red Security Gateway. What are the correct steps to enable CoreXL?
A. SSH to Red Security Gateway, run cpconfig> select Configure Check Point CoreXL > exit cpconfig> reboot the Security Gateway
B. Open the SmartDashboard, Open the Red Check Point Object, select ClusterXL, check the CoreXL box, and push policy
C. Open the SmartDashboard, Open the Red Check Point Object, select Optimizations, check the CoreXL box, and push policy
D. SSH to Red Security Gateway, run cpconfig> select Configure Check Point CoreXL > enable CoreXL > exit cpconfig> reboot the Security Gateway
Answer: D

NO.18 John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to a set of designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.
He has received a new laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop with a static IP (10.0.0.19).

He wants to move around the organization and continue to have access to the HR Web Server. To make this scenario work, the IT administrator:
1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources, and installs the policy.
2) Adds an access role object to the Firewall Rule Base that lets John Adams access the HR Web Server from any machine and from any location and installs policy.
John plugged in his laptop to the network on a different network segment and was not able to connect to the HR Web server. What is the next BEST troubleshooting step?
A. Install the Identity Awareness Agent
B. Set static IP to DHCP
C. Investigate this as a network connectivity issue
D. After enabling Identity Awareness, reboot the gateway
Answer: B

NO.19 Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?
A. Time object to a rule to make the rule active only during specified times.
B. The rule base can be built of layers, each containing a set of the security rules. Layers are inspected in the order in which they are defined, allowing control over the rule base flow and which security functionalities take precedence.
C. Sub Policies are sets of rules that can be created and attached to specific rules. If the rule is matched, inspection will continue in the sub policy attached to it rather than in the next rule
D. Limits the upload and download throughout for streaming media in the company to 1 Gbps.
Answer: B

NO.20 What processes does CPM control?
A. web_services, dle_server and object_Store
B. web-services, CPMI process, DLEserver, CPM process
C. Object-Store, Database changes, CPM Process and web-services
D. DLEServer, Object-Store, CP Process and database changes
Answer: A

NO.21 What is Check Point's CoreXL?
A. Multiple core interfaces on the device to accelerate traffic
B. Multi Core support for Firewall Inspection
C. A way to synchronize connections across cluster members
D. TCP-18190
Answer: B

NO.22 To fully enable Dynamic Dispatcher on a Security Gateway:
A. Using cpconfig, upodate the Dynamic Dispatcher value to "full" under the CoreXl menu
B. run fw ctl multik set_mode 9 in Expert mode and then reboot
C. run fw ctl multik set_mode 1 in Expert mode and then reboot

D. Edit /proc/interrupts to include multik set_mode 1 at the bottom of the file, save, and reboot
Answer: B

NO.23 You are the Security Administrator for MegaCorp. A Check Point firewall is installed and in use on a platform using GAiA.
You have trouble configuring the speed and duplex settings of your Ethernet interfaces.
Which of the following commands can be used in CLISH to configure the speed and duplex settings of an Ethernet interface and will survive a reboot? Give the BEST answer.
A. ifconfig -a
B. set interface <options>
C. mii_tool
D. ethtool
Answer: B

NO.24 Which web services protocol is used to communicate to the Check Point R80 identity Awareness Web APi?
A. SOAP
B. REST
C. XLANG
D. XML-RPC
Answer: B
The Identity Web API uses the REST protocol over SSL. The requests and responses are HTTP and in JSON format.

NO.25 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. 18184
B. 18210
C. 18191
D. 257
Answer: A