Check Point Certified Security Expert (CCSE)

Exam 156-315.80
Check Point Security Expert R80.1 (CCSE)

Version 14.25 (246 Questions)

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT CERTIFIED
SECURITY EXPERT
CCSE

NO.1 Fill in the blank: Identity Awareness AD-Query is using the Microsoft _____ API to learn users
from AD.
A. WMI
B. Eventvwr
C. XML
D. Services.msc
Answer: A

NO.2 With Mobile Access enabled, administrators select the web-based and native applications that can be accessed
by remote users and define the actions that users can perform the applications. Mobile Access encrypts all
traffic using:
A. HTTPS for web-based applications and 3DES or RC4 algorithm for native applications. For end users to
access the native applications, they need to install the SSL. Network Extender.
B. HTTPS for web-based applications and AES or RSA algorithm for native applications. For end users to
access the native application, they need to install the SSL. Network Extender.
C. HTTPS for web-based applications and 3DES or RC4 algorithm for native applications. For end users to
access the native applications, no additional software is required.
D. HTTPS for web-based applications and AES or RSA algorithm for native applications. For end users to
access the native application, no additional software is required.
Answer: A

NO.3 You need to change the number of firewall Instances used by CoreXL. How can you achieve this goal?
A. edit fwaffinity.conf; reboot required
B. cpconfig; reboot required
C. edit fwaffinity.conf; reboot not required
D. cpconfig; reboot not required
Answer: B

NO.4 Connections to the Check Point R80 Web API use what protocol?
A. HTTPS
B. RPC
C. VPN
D. SIC
Answer: A

NO.5 Which command lists all tables in Gaia?

A. fw tab -t
B. fw tab -list
C. fw-tab -s
D. fw tab -1
Answer: C

NO.6 Your manager asked you to check the status of SecureXL, and its enable templates and features, what
command will you use to provide such information to manager?
A. fw accel stat
B. fwaccel stat
C. fw acces stats
D. fwaccel stats
Answer: B

NO.7 When installing a dedicated R80 SmartEvent server. What is the recommended size of the root partition?
A. Any size
B. Less than 20GB
C. More than 10GB and less than 20GB
D. At least 20GB
Answer: D

NO.8 Which one of the following is true about Threat Emulation?
A. Takes less than a second to complete
B. Works on MS Office and PDF files only
C. Always delivers a file
D. Takes minutes to complete (less than 3 minutes)
Answer: D

NO.9 Which of the following is a new R80.10 Gateway feature that had not been available in R77.X and older?
A. 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.
B. Limits the upload and download throughput for streaming media in the company to 1 Gbps.
C. Time object to a rule to make the rule active only during specified times.
D. Sub Policies ae 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.
Answer: D

NO.10 After making modifications to the $CVPNDIR/conf/cvpnd.C file, how would you restart the daemon?
A. cvpnd_restart
B. cvpnd_restart
C. cvpnd restart
D. cvpnrestart
Answer: B

NO.11 Using mgmt_cli, what is the correct syntax to import a host object called Server_1 from the CLI?
A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
B. mgmt_cli add host name "Server_1" ip-address "10.15.123.10" --format json
C. mgmt_cli add object-host "Server_1" ip-address "10.15.123.10" --format json
D. mgmt._cli add object "Server-1" ip-address "10.15.123.10" --format json
Answer: B
Explanation
Example:
mgmt_cli add host name "New Host 1" ip-address "192.0.2.1" --format json
* "--format json" is optional. By default the output is presented in plain text.

NO.12 In the Firewall chain mode FFF refers to:
A. Stateful Packets
B. No Match
C. All Packets
D. Stateless Packets
Answer: C

NO.13 Advanced Security Checkups can be easily conducted within:
A. Reports
B. Advanced
C. Checkups
D. Views
E. Summary
Answer: A

NO.14 Under which file is the proxy arp configuration stored?
A. $FWDIR/state/proxy_arp.conf on the management server
B. $FWDIR/conf/local.arp on the management server
C. $FWDIR/state/_tmp/proxy.arp on the security gateway
D. $FWDIR/conf/local.arp on the gateway
Answer: D

NO.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 each 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.
Answer: A

NO.16 In ClusterXL Load Sharing Multicast Mode:
A. only the primary member received packets sent to the cluster IP address
B. only the secondary member receives packets sent to the cluster IP address
C. packets sent to the cluster IP address are distributed equally between all members of the cluster
D. every member of the cluster received all of the packets sent to the cluster IP address
Answer: D

NO.17 Which TCP-port does CPM process listen to?
A. 18191
B. 18190
C. 8983
D. 19009
Answer: D

NO.18 The CPD daemon is a Firewall Kernel Process that does NOT do which of the following?
A. Secure Internal Communication (SIC)
B. Restart Daemons if they fail
C. Transfers messages between Firewall processes
D. Pulls application monitoring status
Answer: D

NO.19 Which statement is correct about the Sticky Decision Function?
A. It is not supported with either the Performance pack of a hardware based accelerator card
B. Does not support SPI's when configured for Load Sharing
C. It is automatically disabled if the Mobile Access Software Blade is enabled on the cluster
D. It is not required L2TP traffic
Answer: A

NO.20 Which of the following commands shows the status of processes?
A. cpwd_admin -l
B. cpwd -l
C. cpwd admin_list
D. cpwd_admin list
Answer: D

NO.21 The essential means by which state synchronization works to provide failover in the event an active member
goes down, _____ is used specifically for clustered environments to allow gateways to report their
own state and learn about the states of other members in the cluster.
A. ccp
B. cphaconf
C. cphad
D. cphastart
Answer: A

NO.22 John is using Management HA. Which Smartcenter should be connected to for making changes?
A. secondary Smartcenter
B. active Smartenter
C. connect virtual IP of Smartcenter HA
D. primary Smartcenter
Answer: B

NO.23 What happen when IPS profile is set in Detect Only Mode for troubleshooting?
A. It will generate Geo-Protection traffic
B. Automatically uploads debugging logs to Check Point Support Center
C. It will not block malicious traffic
D. Bypass licenses requirement for Geo-Protection control
Answer: C
Explanation
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.

NO.24 During inspection of your Threat Prevention logs you find four different computers having one event each
with a Critical Severity. Which of those hosts should you try to remediate first?
A. Host having a Critical event found by Threat Emulation
B. Host having a Critical event found by IPS
C. Host having a Critical event found by Antivirus
D. Host having a Critical event found by Anti-Bot
Answer: D

NO.25 You are investigating issues with to gateway cluster members are not able to establish the first initial cluster
synchronization. What service is used by the PWO daemon to do a Full Synchronization?
A. TCP port 443
B. TCP port 257
C. TCP port 256
D. UDP port 8116
Answer: C

NO.26 For best practices, what is the recommended time for automatic unlocking of locked admin accounts?
A. 20 minutes
B. 15 minutes
C. Admin account cannot be unlocked automatically
D. 30 minutes at least
Answer: D

NO.27 Which two of these Check Point Protocols are used by SmartEvent Processes?
A. ELA and CPD
B. FWD and LEA
C. FWD and CPLOG
D. ELA and CPLOG
Answer: D

NO.28 During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection
and are rejected by the rule definition, packets are:
A. Dropped without sending a negative acknowledgment
B. Dropped without logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment
Answer: D

NO.29 What is the purpose of extended master key extension/session hash?
A. UDP VOIP protocol extension
B. In case of TLS1.x it is a prevention of a Man-in-the-Middle attack/disclosure of the client-server communication
C. Special TCP handshaking extension
D. Supplement DLP data watermark
Answer: B

NO.30 Which command shows the current connections distributed by CoreXL FW instances?
A. fw ctl multik stat

B. fw ctl affinity -l
C. fw ctl instances -v
D. fw ctl iflist
Answer: A

NO.31 Which of the following will NOT affect acceleration?
A. Connections destined to or originated from the Security gateway
B. A 5-tuple match
C. Multicast packets
D. Connections that have a Handler (ICMP, FTP, H.323, etc.)
Answer: B

NO.32 Which GUI client is supported in R80?
A. SmartProvisioning
B. SmartView Tracker
C. SmartView Monitor
D. SmartLog
Answer: C

NO.33 What is the difference between SSL VPN and IPSec VPN?
A. IPSec VPN does not require installation of a resilient VPN client.
B. SSL VPN requires installation of a resident VPN client.
C. SSL VPN and IPSec VPN are the same.
D. IPSec VPN requires installation of a resident VPN client and SSL VPN requires only an installed Browser.
Answer: D

NO.34 Automation and Orchestration differ in that:
A. Automation relates to codifying tasks, whereas orchestration relates to codifying processes.
B. Automation involves the process of coordinating an exchange of information through web service interactions such as XML and JSON, but orchestration does not involve processes.
C. Orchestration is concerned with executing a single task, whereas automation takes a series of tasks and
puts them all together into a process workflow.
D. Orchestration relates to codifying tasks, whereas automation relates to codifying processes.
Answer: A

NO.35 Which statement is true regarding redundancy?
A. System Administrators know their cluster has failed over and can also see why it failed over by using
the cphaprob -f if command.
B. ClusterXL offers three different Load Sharing solutions: Unicast, Broadcast, and Multicast.
C. Machines in a ClusterXL High Availability configuration must be synchronized.

D. Both ClusterXL and VRRP are fully supported by Gaia and available to all Check Point appliances, open servers, and virtualized environments.
Answer: D

NO.36 What is the SandBlast Agent designed to do?
A. Performs OS-level sandboxing for SandBlast Cloud architecture
B. Ensure the Check Point SandBlast services is running on the end user's system
C. If malware enters an end user's system, the SandBlast Agent prevents the malware from spreading with
the network
D. Clean up email sent with malicious attachments
Answer: C

NO.37 What API command below creates a new host with the name "New Host" and IP address of "192.168.0.10"?
A. new host name "New Host" ip-address "192.168.0.10"
B. set host name "New Host" ip-address "192.168.0.10"
C. create host name "New Host" ip-address "192.168.0.10"
D. add host name "New Host" ip-address "192.168.0.10"
Answer: D

NO.38 SmartConsole R80 requires the following ports to be open for SmartEvent R80 management:
A. 19090,22
B. 19190,22
C. 18190,80
D. 19009,443
Answer: D

NO.39 How many images are included with Check Point TE appliance in Recommended Mode?
A. 2(OS) images
B. images are chosen by administrator during installation
C. as many as licensed for
D. the most new image
Answer: A

NO.40 You have existing dbedit scripts from R77. Can you use them with R80.10?
A. dbedit is not supported in R80.10
B. dbedit is fully supported in R80.10
C. You can use dbedit to modify threat prevention or access policies, but not create or modify layers
D. dbedit scripts are being replaced by mgmt_cli in R80.10
Answer: D

NO.41 What is not a component of Check Point SandBlast?

A. Threat Emulation
B. Threat Simulator
C. Threat Extraction
D. Threat Cloud
Answer: B

NO.42 What command verifies that the API server is responding?
A. api stat
B. api status
C. show api_status
D. app_get_status
Answer: B

NO.43 When an encrypted packet is decrypted, where does this happen?
A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported
Answer: A

NO.44 Check Point recommends configuring Disk Space Management parameters to delete old log entries when
available disk space is less than or equal to?
A. 50%
B. 75%
C. 80%
D. 15%
Answer: D

NO.45 To help SmartEvent determine whether events originated internally you must define using the Initial Settings
under General Settings in the Policy Tab. How many options are available to calculate the traffic direction?
A. 5 Network; Host; Objects; Services; API
B. 3 Incoming; Outgoing; Network
C. 2 Internal; External
D. 4 Incoming; Outgoing; Internal; Other
Answer: D

NO.46 When simulating a problem on ClusterXL cluster with cphaprob -d STOP -s problem -t 0 register, to initiate a
failover on an active cluster member, what command allows you remove the problematic state?
A. cphaprob -d STOP unregister

B. cphaprob STOP unregister
C. cphaprob unregister STOP
D. cphaprob -d unregister STOP
Answer: A

NO.47 VPN Link Selection will perform the following when the primary VPN link goes down?
A. The Firewall will drop the packets.
B. The Firewall can update the Link Selection entries to start using a different link for the same tunnel.
C. The Firewall will send out the packet on all interfaces.
D. The Firewall will inform the client that the tunnel is down.
Answer: B

NO.48 What processes does CPM control?
A. Object-Store, Database changes, CPM Process and web-services
B. web-services, CPMI process, DLEserver, CPM process
C. DLEServer, Object-Store, CP Process and database changes
D. web_services, dle_server and object_Store
Answer: D

NO.49 SSL Network Extender (SNX) is a thin SSL VPN on-demand client that is installed on the remote user's
machine via the web browser. What are the two modes of SNX?
A. Application and Client Service
B. Network and Application
C. Network and Layers
D. Virtual Adapter and Mobile App
Answer: B

NO.50 What is correct statement about Security Gateway and Security Management Server failover in Check Point
R80.X in terms of Check Point Redundancy driven solution?
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 a manual 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 an automatic procedure.
Answer: A