Checkpoint.Pre.156-315.81.50q - DEMO

Number: 156-315.81
Passing Score: 800
Time Limit: 120 min

Exam Code: 156-315.81
Exam Name: Check Point Certified Security Expert R81
Website: https://VCEup.com/
Free Exam: https://vceup.com/exam-156-315-81/

QUESTION 1
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
SecureXL improves non-encrypted firewall traffic throughput and encrypted VPN traffic throughput.

A. This statement is true because SecureXL does improve all traffic.
B. This statement is false because SecureXL does not improve this traffic but CoreXL does.
C. This statement is true because SecureXL does improve this traffic.
D. This statement is false because encrypted traffic cannot be inspected.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SecureXL improved non-encrypted firewall traffic throughput, and encrypted VPN traffic throughput, by nearly an order-of-magnitude- particularly for small packets flowing in long duration connections.
Reference:

QUESTION 3
Which command gives us a perspective of the number of kernel tables?

A. fw tab -t
B. fw tab -s
C. fw tab -n
D. fw tab -k

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
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

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation: esting a failover in a controlled manner using following command; # cphaprob -d STOP -s problem -t 0 register This will register a problem state on the cluster member this was entered on; If you then run; # cphaprob list this will show an entry named STOP. to remove this problematic register run following; # cphaprob -d STOP unregister
Reference:

QUESTION 5
How would you deploy TE250X Check Point appliance just for email traffic and in-line mode without a Check Point Security Gateway?

A. Install appliance TE250X on SpanPort on LAN switch in MTA mode.
B. Install appliance TE250X in standalone mode and setup MTA.
C. You can utilize only Check Point Cloud Services for this scenario.
D. It is not possible, always Check Point SGW is needed to forward emails to SandBlast appliance.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
What is the main difference between Threat Extraction and Threat Emulation?

A. Threat Emulation never delivers a file and takes more than 3 minutes 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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
When Dynamic Dispatcher is enabled, connections are assigned dynamically with the exception of:

A. Threat Emulation
B. HTTPS
C. QOS
D. VoIP

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
SandBlast offers flexibility in implementation based on their individual business needs. What is an option for deployment of Check Point SandBlast Zero-Day Protection?

A. Smart Cloud Services
B. Load Sharing Mode Services
C. Threat Agent Solution
D. Public Cloud Services

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
Which of the following is NOT a component of Check Point Capsule?

A. Capsule Docs
B. Capsule Cloud
C. Capsule Enterprise
D. Capsule Workspace

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
What is the purpose of Priority Delta in VRRP?

A. When a box up, Effective Priority = Priority + Priority Delta
B. When an Interface is up, Effective Priority = Priority + Priority Delta
C. When an Interface fail, Effective Priority = Priority – Priority Delta
D. When a box fail, Effective Priority = Priority – Priority Delta

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Each instance of VRRP running on a supported interface may monitor the link state of other interfaces. The monitored interfaces do not have to be running VRRP.
If a monitored interface loses its link state, then VRRP will decrement its priority over a VRID by the specified delta value and then will send out a new VRRP HELLO packet. If the new effective priority is less than the priority a backup platform has, then the backup platform will beging to send out its own HELLO packet.
Once the master sees this packet with a priority greater than its own, then it releases the VIP.
Reference:

QUESTION 11
Which statements below are CORRECT regarding Threat Prevention profiles in SmartDashboard?

A. You can assign only one profile per gateway and a profile can be assigned to one rule Only.
B. You can assign multiple profiles per gateway and a profile can be assigned to one rule only.
C. You can assign multiple profiles per gateway and a profile can be assigned to one or more rules.
D. You can assign only one profile per gateway and a profile can be assigned to one or more rules.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 12
Using ClusterXL, what statement is true about the Sticky Decision Function?

A. Can only be changed for Load Sharing implementations
B. All connections are processed and synchronized by the pivot
C. Is configured using cpconfig
D. Is only relevant when using SecureXL

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 13
What is the name of the secure application for Mail/Calendar for mobile devices?

A. Capsule Workspace
B. Capsule Mail
C. Capsule VPN
D. Secure Workspace

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 14
Where do you create and modify the Mobile Access policy in R81?

A. SmartConsole
B. SmartMonitor
C. SmartEndpoint
D. SmartDashboard

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
SmartConsole R81 requires the following ports to be open for SmartEvent R81 management:

A. 19090,22
B. 19190,22
C. 18190,80
D. 19009,443

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Which configuration file contains the structure of the Security Server showing the port numbers, corresponding protocol name, and status?

A. $FWDIR/database/fwauthd.conf
B. $FWDIR/conf/fwauth.conf
C. $FWDIR/conf/fwauthd.conf
D. $FWDIR/state/fwauthd.conf

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
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”

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
As a valid Mobile Access Method, what feature provides Capsule Connect/VPN?

A. That is used to deploy the mobile device as a generator of one-time passwords for authenticating to an RSA Authentication Manager.
B. Fill Layer4 VPN –SSL VPN that gives users network access to all mobile applications.
C. Full Layer3 VPN –IPSec VPN that gives users network access to all mobile applications.
D. You can make sure that documents are sent to the intended recipients only.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 19
You find one of your cluster gateways showing “Down” when you run the “cphaprob stat” command.
You then run the “clusterXL_admin up” on the down member but unfortunately the member continues to show down. What command do you run to determine the cause?

A. cphaprob –f register
B. cphaprob –d –s report
C. cpstat –f all
D. cphaprob –a list

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
In SmartEvent, what are the different types of automatic reactions that the administrator can configure?

A. Mail, Block Source, Block Event Activity, External Script, SNMP Trap
B. Mail, Block Source, Block Destination, Block Services, SNMP Trap
C. Mail, Block Source, Block Destination, External Script, SNMP Trap
D. Mail, Block Source, Block Event Activity, Packet Capture, SNMP Trap

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 21
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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.
Reference:

QUESTION 22
What are the steps to configure the HTTPS Inspection Policy?

A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard
B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy
C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy
D. Go to Application&url filtering blade > Https Inspection > Policy

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
You want to store the GAIA configuration in a file for later reference. What command should you use?

A. write mem <filename>
B. show config –f <filename>
C. save config –o <filename>
D. save configuration <filename>

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
How do Capsule Connect and Capsule Workspace differ?

A. Capsule Connect provides a Layer3 VPN. Capsule Workspace provides a Desktop with usable applications.
B. Capsule Workspace can provide access to any application.
C. Capsule Connect provides Business data isolation.
D. Capsule Connect does not require an installed application at client.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
John detected high load on sync interface. Which is most recommended solution?

A. For short connections like http service – delay sync for 2 seconds
B. Add a second interface to handle sync traffic
C. For short connections like http service – do not sync
D. For short connections like icmp service – delay sync for 2 seconds

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Which of these is an implicit MEP option?

A. Primary-backup
B. Source address based
C. Round robin
D. Load Sharing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 27
You have existing dbedit scripts from R77. Can you use them with R81.10?

A. dbedit is not supported in R81.10
B. dbedit is fully supported in R81.10

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 R81.10

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 28
Which Remote Access Client does not provide an Office-Mode Address?

A. SecuRemote
B. Endpoint Security Suite
C. Endpoint Security VPN
D. Check Point Mobile

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 29
What is the command to see cluster status in cli expert mode?

A. fw ctl stat
B. clusterXL stat
C. clusterXL status
D. cphaprob stat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which Check Point daemon monitors the other daemons?

A. fwm
B. cpd
C. cpwd
D. fwssd

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 31

Which command is used to display status information for various components?

A. show all systems
B. show system messages
C. sysmess all
D. show sysenv all

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 32
What are the blades of Threat Prevention?

A. IPS, DLP, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction
B. DLP, AntiVirus, QoS, AntiBot, Sandblast Threat Emulation/Extraction
C. IPS, AntiVirus, AntiBot
D. IPS, AntiVirus, AntiBot, Sandblast Threat Emulation/Extraction

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 33
For Management High Availability, which of the following is NOT a valid synchronization status?

A. Collision
B. Down
C. Lagging
D. Never been synchronized

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 34
Can multiple administrators connect to a Security Management Server at the same time?

A. No, only one can be connected
B. Yes, all administrators can modify a network object at the same time
C. Yes, every administrator has their own username, and works in a session that is independent of other administrators.
D. Yes, but only one has the right to write.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 35
Which process is available on any management product and on products that require direct GUI access, such as SmartEvent and provides GUI client communications, database manipulation, policy compilation and Management HA synchronization?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Firewall Management (fwm) is available on any management product, including Multi-Domain and on products that requite direct GUI access, such as SmartEvent, It provides the following:
– GUI Client communication
– Database manipulation
– Policy Compilation
– Management HA sync

QUESTION 36
To add a file to the Threat Prevention Whitelist, what two items are needed?

A. File name and Gateway
B. Object Name and MD5 signature
C. MD5 signature and Gateway
D. IP address of Management Server and Gateway

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 37
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
What information is NOT collected from a Security Gateway in a Cpinfo?

A. Firewall logs

B. Configuration and database files
C. System message logs
D. OS and network statistics

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 39
SandBlast appliances can be deployed in the following modes:

A. using a SPAN port to receive a copy of the traffic only
B. detect only
C. inline/prevent or detect
D. as a Mail Transfer Agent and as part of the traffic flow only

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enabled which path is handling the traffic?

A. Slow Path
B. Medium Path
C. Fast Path
D. Accelerated Path

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 41
The Correlation Unit performs all but the following actions:

A. Marks logs that individually are not events, but may be part of a larger pattern to be identified later.
B. Generates an event based on the Event policy.
C. Assigns a severity level to the event.
D. Takes a new log entry that is part of a group of items that together make up an event, and adds it to an ongoing event.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 42
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
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.)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
The following command is used to verify the CPUSE version:

A. HostName:0>show installer status build
B. [Expert@HostName:0]#show installer status
C. [Expert@HostName:0]#show installer status build
D. HostName:0>show installer build

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 45
How do you enable virtual mac (VMAC) on-the-fly on a cluster member?

A. cphaprob set int fwha_vmac_global_param_enabled 1
B. clusterXL set int fwha_vmac_global_param_enabled 1
C. fw ctl set int fwha_vmac_global_param_enabled 1
D. cphaconf set int fwha_vmac_global_param_enabled 1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 46
To accelerate the rate of connection establishment, SecureXL groups all connection that match a particular service and whose sole differentiating element is the source port. The type of grouping enables even the very first packets of a TCP handshake to be accelerated. The first packets of the first connection on the same service will be forwarded to the Firewall kernel which will then create a template of the connection. Which of the these is NOT a SecureXL template?

A. Accept Template
B. Deny Template
C. Drop Template
D. NAT Template

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Reference:

QUESTION 47
Which of the following is NOT a type of Check Point API available in R81.x?

A. Identity Awareness Web Services
B. OPSEC SDK
C. Mobile Access
D. Management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 48
When an encrypted packet is decrypted, where does this happen?

A. Security policy
B. Inbound chain
C. Outbound chain
D. Decryption is not supported

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
John is using Management H

A. Which Smartcenter should be connected to for making changes?
B. secondary Smartcenter
C. active Smartenter
D. connect virtual IP of Smartcenter HA
E. primary Smartcenter

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 50
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. fwd
B. fwm
C. cpd
D. cpwd

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation: