Vendor: Check Point

Exam Code: 156-315.81

Exam Name: Check Point Certified Security Expert R81

Version: DEMO

QUESTION 1
Which member of a high-availability cluster should be upgraded first in a Zero downtime upgrade?

A. The Standby Member
B. The Active Member
C. The Primary Member
D. The Secondary Member

Answer: A
Explanation:
During the upgrade procedure, standby members are upgraded first. When upgrade on the final active member begins, the active member fails over to the standby member (or members, depending on the deployment: High Availability or Load Sharing). At this point, since connection tables between cluster members are not synced, all open connections are lost. Only a full connectivity upgrade (between minor versions) preserves open connections.

QUESTION 2
Packet acceleration (SecureXL) identifies connections by several attributes. Which of the attributes is NOT used for identifying connection?

A. Source Address
B. Destination Address
C. TCP Acknowledgement Number
D. Source Port

Answer: C
Explanation:
Connections are identified by the 5 tuple attributes: source address, destination address, source port, destination port, protocol. When the packets in a connection match all the 5 tuple attributes, the traffic flow can be processed on the accelerated path.

QUESTION 3
Which of the following is NOT an attribute of packet acceleration?

A. Source address
B. Protocol
C. Destination port
D. VLAN tag

Answer: D
Explanation:
Connections are identified by the 5 tuple attributes: source address, destination address, source port, destination port, protocol. When the packets in a connection match all the 5 tuple attributes, the traffic flow can be processed on the accelerated path.

QUESTION 4
CoreXL is NOT supported when one of the following features is enabled: (Choose three)

A. Route-based VPN
B. IPS

C. IPv6
D. Overlapping NAT

Answer: ACD
Explanation:
CoreXL does not support Check Point Suite with these features:
Check Point QoS (Quality of Service)
Route-based VPN
IPv6 on IPSO
Overlapping NAT

QUESTION 5
Which one of these features is NOT associated with the Check Point URL Filtering and Application Control Blade?

A. Detects and blocks malware by correlating multiple detection engines before users are affected.
B. Configure rules to limit the available network bandwidth for specified users or groups.
C. Use UserCheck to help users understand that certain websites are against the company's security policy.
D. Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels.

Answer: A
Explanation:
https://sc1.checkpoint.com/documents/R76/CP_R76_AppControl_WebAdmin/60902.htm

QUESTION 6
What is a feature that enables VPN connections to successfully maintain a private and secure VPN session without employing Stateful Inspection?

A. Stateful Mode
B. VPN Routing Mode
C. Wire Mode
D. Stateless Mode

Answer: C
Explanation:
Wire Mode is a VPN-1 NGX feature that enables VPN connections to successfully fail over, bypassing Security Gateway enforcement. This improves performance and reduces downtime. Based on a trusted source and destination, Wire Mode uses internal interfaces and VPN Communities to maintain a private and secure VPN session, without employing Stateful Inspection. Since Stateful Inspection no longer takes place, dynamic-routing protocols that do not survive state verification in non-Wire Mode configurations can now be deployed. The VPN connection is no different from any other connections along a dedicated wire, thus the meaning of "Wire Mode".

QUESTION 7
The Firewall kernel is replicated multiple times, therefore:

A. The Firewall kernel only touches the packet if the connection is accelerated
B. The Firewall can run different policies per core

C. The Firewall kernel is replicated only with new connections and deletes itself once the connection times out
D. The Firewall can run the same policy on all cores.

Answer: D
Explanation:
On a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated copy, or instance, runs on one processing core. These instances handle traffic concurrently, and each instance is a complete and independent inspection kernel. When CoreXL is enabled, all the kernel instances in the Security Gateway process traffic through the same interfaces and apply the same security policy.

QUESTION 8
An Account Unit is the interface between the _____ and the _____.

A. Users, Domain
B. Gateway, Resources
C. System, Database
D. Clients, Server

Answer: D
Explanation:
When deployed with a SmartDirectory (LDAP) server, the Check Point Security Management (SmartCenter Server) and Security Gateways, function as SmartDirectory (LDAP) clients. An Account Unit is the interface that allows interaction between these entities and the SmartDirectory (LDAP) server(s). Each Account Unit represents one or more branches of the information maintained on the SmartDirectory (LDAP) server.

QUESTION 9
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

Answer: D
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 10
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:
mgmt_cli add host name "New Host 1" ip-address "192.0.2.1" --format json ?;--format jso"; is optional. By default the output is presented in plain text.
Reference:
https://sc1.checkpoint.com/documents/latest/APIs/index.html#cli/add-host~v1.1%20

QUESTION 11
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

Answer: C
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.

QUESTION 12
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
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

QUESTION 13

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.

Answer: C
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.

QUESTION 14
Fill in the blank: The R81 utility fw monitor is used to troubleshoot _____.

A. User data base corruption
B. LDAP conflicts
C. Traffic issues
D. Phase two key negotiations

Answer: C
Explanation:
Check Point's FW Monitor is a powerful built-in tool for capturing network traffic at the packet level. The FW Monitor utility captures network packets at multiple capture points along the FireWall inspection chains. These captured packets can be inspected later using the WireShark

QUESTION 15
What SmartEvent component creates events?

A. Consolidation Policy
B. Correlation Unit
C. SmartEvent Policy
D. SmartEvent GUI

Answer: B
Explanation:
https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEvent_AdminGuide/17401.htm

QUESTION 16
Which command collects diagnostic data for analyzing customer setup remotely?

A. cpinfo
B. migrate export
C. sysinfo
D. cpview

Answer: A
Explanation:

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.

QUESTION 17
Which Check Point daemon monitors the other daemons?

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

Answer: C
Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

QUESTION 18
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

Answer: A
Explanation:
https://www.checkpoint.com/products/next-generation-threat-prevention/

QUESTION 19
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

Answer: A
Explanation:
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92739

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**