Vendor: Check Point

Exam Code: 156-315.71

Exam Name: Check Point Certified Security Expert R71

Version: DEMO

1.You need to publish SecurePlatform routes using the ospf routing protocol. What is the correct command structure, once entering the route command, to implement ospf successfully?
A. Run cpconfig utility to enable ospf routing
B. ip route ospf
ospf network1
ospf network2
C. Enable
Configure terminal
Router ospf [id]
Network [network] [wildmask] area [id]
D. Use DBedit utility to either the objects_5_0.c file
Answer: C

2.Control connections between the Security Management Server and the Gateway are not encrypted by the VPN Community. How are these connections secured?
A. They are encrypted and authenticated using SIC.
B. They are not encrypted, but are authenticated by the Gateway
C. They are secured by PPTP
D. They are not secured.
Answer: D

3.How does a cluster member take over the VIP after a failover event?
A. Ping the sync interface
B. if list -renew
C. Broadcast storm
D. Gratuitous ARP
Answer: D

4.You want to verify that your Check Point cluster is working correctly. Which command line tool can you use?
A. cphaconf state
B. cphaprob state
C. cphainfo-s
D. cphastart -status
Answer: B

5._____is a proprietary Check Point protocol. it is the basis for Check Point ClusterXL inter-module
communication.
A. RDP
B. CCP
C. CKPP
D. HA OPCODE

Answer: B

6.John is configuring a new R71 Gateway cluster but he can not configure the cluster as Third Party IP Clustering because this option is not available in Gateway Cluster Properties: What's happening?
A. John is not using third party hardware as IP Clustering is part of Check Point's IP Appliance
B .Third Party Clustering is not available for R71 Security Gateways.
B. ClusterXL needs to be unselected to permit 3rd party clustering configuration.
C. John has an invalid ClusterXL license.
Answer: C

7.You are MegaCorp Security Administrator. This company uses a firewall cluster, consisting of two cluster members. The cluster generally works well but one day you find that the cluster is behaving strangely. You assume that there is a connectivity problem with the cluster synchronization cluster link (cross-over cable).
Which of the following commands is the best for testing the connectivity of the crossover cable?
A. telnet <IP address of the synchronization interface on the other cluster member>
B. arping <IP address of the synchronization interface on the other cluster member>
C. ifconfig a
D. Ping <IP address of the synchronization interface on the other cluster member>
Answer: B

8.Organizations are sometimes faced with the need to locate cluster members in different geographic locations that are distant from each other. A typical example is replicated data centers whose location is widely separated for disaster recovery purposes.
What are the restrictions of this solution?
A. There are no restrictions.
B. There is one restriction: The synchronization network must guarantee no more than 150 ms latency (ITU Standard G.114).
C. There is one restriction: The synchronization network must guarantee no more than 100 ms latency.
D. There are two restrictions: 1. The synchronization network must guarantee no more than 100ms latency and no more than 5% packet loss. 2. The synchronization network may only include switches and hubs.
Answer: D

9.You are establishing a ClusterXL environment, with the following topology: External interfaces 192.168.10.1 and 192.168.10.2 connect to a VLAN switch. The upstream router connects to the same VLAN switch. Internal interfaces 172.16 10.1 and 172.16.10.2 connect to a hub. 10.10.10.0 is the synchronization network. The Security Management Server is located on the internal network with IP 172.16.10.3. What is the problem with this configuration?
A. There is an IP address conflict

B. The Security Management Server must be in the dedicated synchronization network, not the internal network.

C. The Cluster interface names must be identical across all cluster members.

D. Cluster members cannot use the VLAN switch. They must use hubs.

Answer: B

10.Refer to Exhibit:

Mode	Configuration
A. Legacy Mode High Availability	1. Every member of the cluster receives all packets sent to the cluster IP address, which the load distributed optimally among all cluster members
B. New Mode High Availability	2. Only one machine is active at any time. A failure of the active machine causes a failover to the next highest priority machine in the cluster.
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 the other machines in the cluster, implementing both load sharing and redundancy

Match the ClusterXL Modes with their configurations

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

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

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

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

Answer: C

11.Check point Clustering protocol, works on:

A. UDP 8116

B. UDP 500

C. TCP 8116

D. TCP 19864

Answer: A

12.What command will allow you to disable sync on a cluster firewall member?

A. fw ctl setsync 0

B. fw ctl sysnstat stop

C. fw ctl sysnstat off

D. fw ctl setsyns off

Answer: D

13.Which of the following statements about the Port Scanning feature of IPS is TRUE?

A. The default scan detection is when more than 500 open inactive ports are open for a period of 120 seconds.

B. The Port Scanning feature actively blocks the scanning, and sends an alert to SmartView Monitor.
C. Port Scanning does not block scanning; it detects port scans with one of three levels of detection sensitivity.
D. When a port scan is detected, only a log is issued, never an alert.
Answer: C

14.Which procedure creates a new administrator in SmartWorkflow?
A. Run cpconfig, supply the Login Name. Profile Properties, Name, Access Applications and Permissions.
B. In SmartDashboard, click SmartWorkflow / Enable SmartWorkflow and the Enable SmartWorkflow wizard will start. Supply the Login Name, Profile Properties, Name, Access Applications and Permissions when prompted.
C. On the Provider-1 primary MDS, run cpconfig, supply the Login Name, Profile Properties, Name, Access Applications and Permissions.
D. In SmartDashboard, click Users and Administrators right click Administrators / New Administrator and supply the Login Name. Profile Properties, Name, Access Applications and Permissions.
Answer: D

15.When you check Web Server in a host-node object, what happens to the host?
A. The Web server daemon is enabled on the host.
B. More granular controls are added to the host, in addition to Web Intelligence tab settings.
C. You can specify allowed ports in the Web server's node-object properties. You then do not need to list all allowed ports in the Rule Base.
D. IPS Web Intelligence is enabled to check on the host.
Answer: B

16.Which external user authentication protocols are supported in SSL VPN?
A. LDAP, Active Directory, SecurID
B. DAP, SecurID, Check Point Password, OS Password, RADIUS, TACACS
C. LDAP, RADIUS, Active Directory, SecurID
D. LDAP, RADIUS, TACACS, SecurID
Answer: B

17.Which of the following commands can be used to stop Management portal services?
A. fw stopportal
B. cpportalstop
C. cpstop / portal
D. smartportalstop
Answer: D

18.Which of the following is NOT a feature of ClusterXL?

A. Enhanced throughput in all ClusterXL modes (2 gateway cluster compared with 1 gateway)
B. Transparent failover in case of device failures
C. Zero downtime for mission-critical environments with State Synchronization
D. Transparent upgrades
Answer: C

19.Which of the following manages Standard Reports and allows the administrator to specify automatic uploads of reports to a central FTP server?
A. Smart Dashboard Log Consolidator
B. Security Management Server
C. Smart Reporter Database
D. Smart Reporter
Answer: D

20.What is a task of the SmartEvent Correlation Unit?
A. Add events to the events database.
B. Look for patterns according to the installed Event Policy.
C. Assign a severity level to an event
D. Display the received events.
Answer: B