

# 156-915.65<sup>Q&As</sup>

Accelerated CCSE NGX R65

## Pass CheckPoint 156-915.65 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/156-915-65.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint  
Official Exam Center

- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers



## QUESTION 1

Which Security Servers can perform authentication tasks, but CANNOT perform content security tasks?

- A. Telnet
- B. HTTP
- C. FTP
- D. SMTP

Correct Answer: A

---

## QUESTION 2

The Check Point ClusterXL mode must synchronize the physical interface IP and MAC addresses on all clustered interfaces

- A. New Mode HA
- B. Legacy Mode HA
- C. Multicast Mode Load Sharing
- D. Pivot Mode Load Sharing

Correct Answer: B

---

## QUESTION 3

Which of these components does NOT require a VPN-1 NGX R65 license?

- A. Check Point Gateway
- B. SmartCenterServer
- C. SmartConsole
- D. SmartUpdate upgrading/patching

Correct Answer: C

---

## QUESTION 4

Which utility allows you to configure the DHCP service on SecurePlatform from the command line?

- A. WebUI

B. cpconfig

C. ifconfig

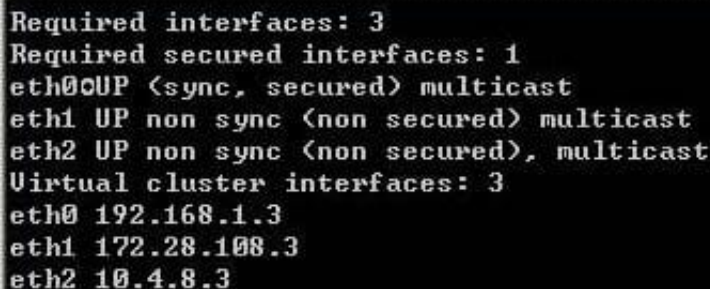
D. sysconfig

Correct Answer: D

---

### QUESTION 5

An NGXR65 HA cluster contains two members with external interfaces 172.28.108.1 and 172.28.108.2. The internal interfaces are 10.4.8.1 and 10.4.8.2. The external cluster VIP address is 172.28.108.3 and the internal cluster VIP address is 10.4.8.3. The synchronization interfaces are 192.168.1.1 and 192.168.1.2. The Security Administrator discovers State Synchronization is not working properly. The cphaprob if command output displays shows: What is causing the State Synchronization problem?



```
Required interfaces: 3
Required secured interfaces: 1
eth0 UP <sync, secured> multicast
eth1 UP non sync <non secured> multicast
eth2 UP non sync <non secured>, multicast
Virtual cluster interfaces: 3
eth0 192.168.1.3
eth1 172.28.108.3
eth2 10.4.8.3
```

A. The synchronization network has been defined as "Network Objective: Cluster + 1st sync" with an IP address 192.168.1.3 defined in the NGX cluster object's topology. This configuration is supported in NGX and therefore the above screenshot is not relevant to the sync problem.

B. The synchronization interface on the individual NGX cluster member object's Topology tab is enabled with "Cluster Interface". Disable this setting.

C. The synchronization network has a cluster VIP address (192.168.1.3) defined in the NGX cluster object's topology. Remove the 192.168.1.3 VIP interface from the cluster topology.

D. Another cluster is using 192.168.1.3 as one of the unprotected interfaces.

Correct Answer: A

---

### QUESTION 6

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Power Gateway. You want to implement Management High Availability (HA). You have a spare machine to configure as the secondary SmartCenter Server. How do you configure the new machine to be the standby SmartCenter Server?

A. Use cpprod\_util to reconfigure the primary SmartCenter Server to become the secondary on the VPN-1 Power Gateway. Install a new primary SmartCenter Server on the spare machine and set to "standby". Synchronize the "active" secondary to the "standby" primary in order to migrate the configuration.

- B. Install the secondary Server on the spare machine. Add the new machine to any network routable to the primary Server. Synchronize the machines.
- C. You cannot configure Management HA, when either the primary or secondary SmartCenter Server is running on a VPN-1 Pro Gateway.
- D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server. Synchronize the machines.

Correct Answer: C

---

#### QUESTION 7

Your bank\\'s distributed VPN-1 NGX R65 installation has Security Gateways up for renewal. Which SmartConsole application will tell you which Security Gateways have licenses that will expire within the next 30 days?

- A. SmartUpdate
- B. SmartViewTracker
- C. SmartDashboard
- D. SmartPortal

Correct Answer: D

---

#### QUESTION 8

What physical machine must have access to the User Center public IP when checking for new packages with SmartUpdate?

- A. SmartUpdate installed SmartCenter Server PC
- B. SmartUpdate GUI PC
- C. VPN-1 Security Gateway getting the new upgrade package
- D. SmartUpdate Repository SQL database Server

Correct Answer: B

---

#### QUESTION 9

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Power Gateway. You want to implement Management High Availability (HA). You have a spare machine to configure as the secondary SmartCenter Server. How do you configure the new machine to be the standby SmartCenter Server?

- A. Use cprod\_util to reconfigure the primary SmartCenter Server to become the secondary on the VPN-1 Power Gateway. Install a new primary SmartCenter Server on the spare machine and set to "standby". Synchronize the "active" secondary to the "standby" primary in order to migrate the configuration.

- B. Install the secondary Server on the spare machine. Add the new machine to any network routable to the primary Server. Synchronize the machines.
- C. You cannot configure Management HA, when either the primary or secondary SmartCenter Server is running on a VPN-1 Pro Gateway.
- D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server. Synchronize the machines.

Correct Answer: C

---

## QUESTION 10

The Check Point ClusterXL mode must synchronize the physical interface IP and MAC addresses on all clustered interfaces

- A. New Mode HA
- B. Legacy Mode HA
- C. Multicast Mode Load Sharing
- D. Pivot Mode Load Sharing

Correct Answer: B

---

## QUESTION 11

If you are experiencing LDAP issues, which of the following should you check?

- A. Connectivity between the NGX gateway and LDAP server
- B. Secure Internal Communications (SIC)
- C. VPN Load Balancing
- D. Overlapping VPN Domains

Correct Answer:

---

## QUESTION 12

How do you block some seldom-used FTP commands, such as CWD, and FIND from passing through the Gateway?

- A. Use FTP Security Server settings in SmartDefense.
- B. Add the restricted commands to the `ftpd.conf` file in the SmartCenter Server.
- C. Configure the restricted FTP commands in the Security Servers screen of the Global properties.
- D. Enable FTP Bounce checking in SmartDefense.

Correct Answer: A

---

## QUESTION 13

When launching SmartDashboard, what information is required to log into VPN-1 NGX R65?

- A. User Name, Password, SmartCenter Server IP
- B. User Name, SmartCenter Server IP, certificate fingerprint file
- C. Password, SmartCenter Server IP, LDAP Server
- D. Password, SmartCenter Server IP

Correct Answer: B

---

## QUESTION 14

Your primary SmartCenter Server is installed on a SecurePlatform Pro machine, which is also a VPN-1 Power Gateway. You want to implement Management High Availability (HA). You have a spare machine to configure as the secondary SmartCenter Server. How do you configure the new machine to be the standby SmartCenter Server?

- A. Use cprod\_util to reconfigure the primary SmartCenter Server to become the secondary on the VPN-1 Power Gateway. Install a new primary SmartCenter Server on the spare machine and set to "standby". Synchronize the "active" secondary to the "standby" primary in order to migrate the configuration.
- B. Install the secondary Server on the spare machine. Add the new machine to any network routable to the primary Server. Synchronize the machines.
- C. You cannot configure Management HA, when either the primary or secondary SmartCenter Server is running on a VPN-1 Pro Gateway.
- D. Install the secondary Server on the spare machine. Add the new machine to the same network as the primary Server. Synchronize the machines.

Correct Answer: C

---

## QUESTION 15

In a Management High Availability (HA) configuration, you can configure synchronization to occur automatically, when

- (1) The Security Policy is installed.
- (2) The Security Policy is saved.
- (3) The Security Administrator logs in to the secondary SmartCenter Server, and changes its status to active.
- (4) A scheduled event occurs.
- (5) The

user database is installed.

Select the BEST response for the synchronization sequence. Choose One:

A.

1,2,3,4

B.

1,2,5

C.

1,2,4

D.

1,3,4

Correct Answer: C

[Latest 156-915.65 Dumps](#)

[156-915.65 PDF Dumps](#)

[156-915.65 Exam Questions](#)