



Vendor: Check Point

Exam Code: 156-915.76

Exam Name: Check Point Certified Security Expert Update
Blade

Version: DEMO

QUESTION 1

To force clients to use integritySecurity Workspace when accessing sensitive applications, the Administrator can configure Connectra:

- A. Via protection levels
- B. To implement integrity Clientless Security
- C. To force the user to re-authenticate at login
- D. Without a special setting. Secure Workspace is automatically configured.

Answer: A

QUESTION 2

The default port for browser access to the Management Portal is

- A. 4433
- B. 4343
- C. 8080
- D. 443

Answer: A

QUESTION 3

In which case is a Sticky Decision Function relevant?

- A. Load Sharing - Unicast
- B. Load Balancing - Forward
- C. High Availability
- D. Load Sharing - Multicast

Answer: D

QUESTION 4

You just upgraded to R71 and are using the IPS Software Blade. You want to enable all critical protections while keeping the rate of false positives very low. How can you achieve this?

- A. The new IPS system is based on policies, but it has no ability to calculate or change the confidence level, so it always has a high rate of false positives.
- B. This can't be achieved; activating any IPS system always causes a high rate of false positives.
- C. The new IPS system is based on policies and gives you the ability to activate all checks with critical severity and a high confidence level.
- D. As in SmartDefense, this can be achieved by activating all the critical checks manually.

Answer: C

QUESTION 5

Refer to the network topology below. You have IPS Software Blades active on the Security Gateways sgldon, sgla, and sgny, but still experience attacks on the Web server in the New York DMZ. How is this possible?

- A. AH of these options are possible.
- B. The attacker may have used a bunch of evasion techniques like using escape sequence instead of cleartext commands. It is also possible that there are entry points not shown in the network layout, like rogue access points.
- C. Since other Gateways do not have IPS activated, attacks may originate from their network without anyone noticing.
- D. An IPS may combine different detection technologies, but is dependent on regular signature updates and well-tuned anomaly algorithms. Even if this is accomplished, no technology can offer 100 % protection.

Answer: C

QUESTION 6

Which of the following is NOT an Smartevent event-triggered Automatic Reaction?

- A. Mail
- B. Block Access
- C. External Script
- D. SNMP Trap

Answer: B

QUESTION 7

Your company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed. Which actions should be taken to achieve that?

- A. (i), (ii) and (iv)
- B. (i), (iii), (iv)
- C. (ii) and (iv)
- D. (i) and (ii)

Answer: C

QUESTION 8

What SmartConsole application allows you to change the Log Consolidation Policy?

- A. SmartReporter
- B. SmartUpdate
- C. SmartEvent Server
- D. Smart Dashboard

Answer: A

QUESTION 9

In configure a client to properly log in to the user portal using a certificate, the Administrator MUST:

- A. Create an internal user in the admin portal.

- B. Install an R71 internal Certificate Authority certificate.
- C. Create a client certificate from Smart Dashboard
- D. Store the client certificate on the SSL VPN Gateway

Answer: C

QUESTION 10

What process manages the dynamic routing protocols (ospf, RIP, etc) on SecurePlatform Pro?

- A. gated
- B. arouted
- C. routerd
- D. There is no separate process, but the Linux default router can take care of that.

Answer: A

QUESTION 11

To change the default port of the Management Portal,

- A. Edit the masters.conf file on the Portal server.
- B. Modify the file cp_httpd_admin.conf.
- C. Run sysconfig and change the management interface
- D. Re-initialize SIC.

Answer: C

QUESTION 12

Where do Gateways managed by SmartProvisioning fetch their assigned profiles?

- A. The Smartview Monitor
- B. The standalone SmartProvisioning server
- C. The Security Management server or CMA
- D. They are fetched locally from the individual device

Answer: C

QUESTION 13

When synchronizing clusters, which of the following statements is NOT true?

- A. Client Auth or Session Auth connections through a cluster member will be lost if the cluster member fails.
- B. The state of connection using resources is maintained by a Security Server, so there connections cannot be synchronized.
- C. Only cluster members running on the same OS platform can be synchronized.
- D. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.

Answer: D

QUESTION 14

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

- A. fw ctl setaync 0
- B. fw ctl syncstat stop
- C. fw ctl syncstat off
- D. fw ctl setsync off

Answer: D

QUESTION 15

By default, a standby Security Management Server is automatically synchronized by an active Security Management Server, when:

- A. The Security Policy is saved.
- B. The Security Policy is installed.
- C. The user database is installed.
- D. The standby Security Management Server starts for the first time.

Answer: A

QUESTION 16

A customer is calling saying one member's status is Down. What will you check?

- A. cphaprob list (verify what critical device is down)
- B. Fw ctl debug m cluster + forward (forwarding layer debug)
- C. tcpdump/snoop (CCP traffic)
- D. fw ctlpstat (check sync)

Answer: A

QUESTION 17

You have a High Availability ClusterXL configuration. Machines are not synchronizing. What happens to connections on failover?

- A. It is not possible to configure High Availability that is not synchronized.
- B. Old connections are lost but can be reestablished.
- C. Connection cannot be established until cluster members are fully synchronized.
- D. Old connections are lost but are automatically recovered whenever the failed machine recovers.

Answer: B

QUESTION 18

When using ClusterXL in load sharing, what method is used by default?

- A. IPs, SPIs
- B. IPs, Ports, SPIs

- C. IPs
- D. IPs, Ports

Answer: C

QUESTION 19

John is configuring a new R17 Gateway cluster but he cannot configure the cluster as Third Party IP Clustering in Gateway Cluster Properties:
What is happening?

- A. John is not using third party hardware as IP Clustering is part of Check Point sIP Appliance.
- B. Third Party Clustering is not available for R71 Security Gateways.
- C. ClusterXL needs to be unselected to permit 3rd party clustering configuration.
- D. John has an invalid ClusterXL license

Answer: C

QUESTION 20

A customer calls saying that a load-sharing cluster shows drops with the error First packet is not SYN. Complete the following sentence. I will recommend:

- A. Change the load on each member.
- B. configuring flush and ack
- C. turning off SDF (Sticky Decision Function)
- D. turning on SDF (Sticky Decision Function)

Answer: D

Thank You for Trying Our Product

Lead2pass 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.lead2pass.com/all-products.html>



Microsoft



ORACLE



CITRIX



JUNIPER
NETWORKS



EMC²
where information lives®

10% Discount Coupon Code: ASTR14