



**Vendor:** Check Point

**Exam Code:** 156-315.71

**Exam Name:** Check Point Certified Security Expert R71

**Version:** DEMO

#### QUESTION 1

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**

#### QUESTION 2

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**

#### QUESTION 3

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**

#### QUESTION 4

Based on the following information, which of the statements below is FALSE?

A DLP Rule Base has the following conditions:

Data Type =Password Protected File

Source=My Organization

Destination=Outside My Organization

Protocol=Any

Action=Ask User

Exception: Data Type=Any,

Source=Research and Development (R&D)

Destination=Pratner1.com

Protocol=Any

All other rules are set to Detect. UserCheck is enabled and installed on all client machines.

- A. When a user from R&D sends an e-mail with a password protected PDF file as an attachment to xyz@partner1.com, he will be prompted by UserCheck.
- B. When a user from Finance sends an e-mail with an encrypted ZIP file as an attachment to. He will be prompted by UserCheck.

- C. Another rule is added: Source = R&D, Destination = partner1.com, Protocol = Any, Action = Inform. When a user from R&D sends an e-mail with an encrypted ZIP file as an attachment to, he will be prompted by UserCheck.
- D. When a user from R&D sends an e-mail with an encrypted ZIP file as an attachment to, he will NOT be prompted by UserCheck.

**Answer: B**

#### QUESTION 5

A VPN Tunnel Interface (VTI) is defined on SecurePlatform Pro as:

```
vpn shell interface add numbered 10.10.0.1 10.10.0.2 "madrid.cp".
```

What do you know about this VTI?

- A. The peer Security Gateway's name is "madrid.cp".
- B. The local Gateway's object name is "madrid.cp".
- C. The VTI name is "madrid.cp".
- D. 10.10.0.1 is the local Gateway's internal interface, and 10.10.0.2 is the internal interface Gateway.

**Answer: A**

#### QUESTION 6

You use the snapshot feature to store your Connectra SSL VPN configuration. What do you expect to find?

- A. Nothing; snapshot is not supported in Connectra SSL VPN.
- B. The management configuration of the current product, on a management or stand-alone machine
- C. A complete image of the local file system
- D. Specified directories of the local file system.

**Answer: C**

#### QUESTION 7

When running DLP Wizard for the first time, which of the following is a mandatory configuration?

- A. Mail Server
- B. E-mail Domain in My Organization
- C. DLP Portal URL
- D. Active Directory

**Answer: B**

#### QUESTION 8

When using Connectra with Endpoint Security Policies, what option is not available when configuring DAT enforcement?

- A. Maximum DAT file version
- B. Maximum DAT file age

- C. Minimum DAT file version
- D. Oldest DAT file timestamp

**Answer: A**

**QUESTION 9**

Which specific R71 GUI would you use to view the length of time a TCP connection was open?

- A. SmartReporter
- B. SmartView Monitor
- C. SmartView Status
- D. SmartView Tracker

**Answer: D**

**QUESTION 10**

What is not available for Express Reports compared to Standard Reports?

- A. Filter
- B. Period
- C. Content
- D. Schedule

**Answer: A**

**QUESTION 11**

Based on the following information, which of the statements below is TRUE?

A DLP Rule Base has the following conditions:

Data Type = Large file (> 500KB)

Source = My Organization

Destination = Free Web Mails

Protocol = Any

Action = Ask User

All other rules are set to Detect. UserCheck is enabled and installed on all client machines.

- A. When a user uploads a 600 KB file to his Yahoo account via Web Mail (via his browser), he will be prompted by UserCheck
- B. When a user sends an e-mail with a small body and 5 attachments, each of 200 KB to, he will be prompted by UserCheck.
- C. When a user sends an e-mail with an attachment larger than 500 KB to, he will be prompted by UserCheck.
- D. When a user sends an e-mail with an attachment larger than 500KB to, he will be prompted by UserCheck.

**Answer: A**

**QUESTION 12**

If Bob wanted to create a Management High Availability configuration, what is the minimum

number of Security Management servers required in order to achieve his goal?

- A. Three
- B. Two
- C. Four
- D. One

**Answer: D**

#### **QUESTION 13**

Which of the following statements is FALSE about the DLP Software Blade and Active Directory (AD) or LDAP?

- A. When a user authenticates in the DLP Portal to view all his unhandled incidents, the portal authenticates the user using only AD/LDAP.
- B. Check Point UserCheck client authentication is based on AD.
- C. For SMTP traffic, each recipient e-mail address is translated using AD/LDAP to a user name and group that is checked vs. the destination column of the DLP rule base.
- D. For SMTP traffic, the sender e-mail address is translated using AD/LDAP to a user name and group that is checked vs. the source column of the DLP rule base.

**Answer: A**

#### **QUESTION 14**

You are running R71 and using the new IPS Software Blade. To maintain the highest level of security, you are doing IPS updates regularly. What kind of problems can be caused by the automatic updates?

- A. None; updates will not add any new security checks causing problematic behaviour on the systems.
- B. None, all new updates will be implemented in Detect only mode to avoid unwanted traffic interruptions. They have to be activated manually later.
- C. None, all the checks will be activated from the beginning, but will only detect attacks and not disturb any non-malicious traffic in the network.
- D. All checks will be activated from the beginning and might cause unwanted traffic outage due to false positives of the new checks and non-RFC compliant self-written applications.

**Answer: B**

#### **QUESTION 15**

Which of the following deployment scenarios CANNOT be managed by Check Point QoS?

- A. Two lines connected to a single router, and the router is connected directly to the Gateway
- B. Two lines connected to separate routers, and each router is connected to separate interfaces on the Gateway
- C. One LAN line and one DMZ line connected to separate Gateway interfaces
- D. Two lines connected directly to the Gateway through a hub

**Answer: A**

**QUESTION 16**

Which method of load balancing describes "Round Robin"?

- A. Assigns service requests to the next server in a series.
- B. Ensures that incoming requests are handled by the server with the fastest response time.
- C. Measures the load on each server to determine which server has the most available resources.
- D. Assigns service requests to servers at random.

**Answer: A**

**QUESTION 17**

David wants to manage hundreds of gateways using a central management tool. What tool would David use to accomplish his goal?

- A. SmartProvisioning
- B. SmartBlade
- C. SmartDashboard
- D. SmartLSM

**Answer: B**

**QUESTION 18**

Which technology is responsible for assembling packet streams and passing ordered data to the protocol parsers in IPS?

- A. Pattern Matcher
- B. Content Management Infrastructure
- C. Accelerated INSPECT
- D. Packet Streaming Layer

**Answer: D**

**QUESTION 19**

You configure a Check Point QoS Rule Base with two rules: an HTTP rule with a weight of 40, and the Default Rule with a weight of 10. If the only traffic passing through your QoS Module is HTTP traffic, what percent of bandwidth will be allocated to the HTTP traffic?

- A. 80%
- B. 40%
- C. 100%
- D. 50%

**Answer: D**

**QUESTION 20**

You configure a Check Point QoS Rule Base with two rules: an H.323 rule with a weight of 10, and the Default Rule with a weight of 10. The H.323 rule includes a per-connection guarantee of 384 Kbps. and a per-connection limit of 512 Kbps. The per-connection guarantee is for four connections, and no additional connections are allowed in the Action properties. If traffic is

passing through the QoS Module matches both rules, which of the following statements is TRUE?

- A. Each H.323 connection will receive at least 512 Kbps of bandwidth.
- B. The H.323 rule will consume no more than 2048 Kbps of available bandwidth.
- C. 50% of available bandwidth will be allocated to the Default Rule.
- D. Neither rule will be allocated more than 10% of available bandwidth.

**Answer: B**

## 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



EMC<sup>2</sup>  
where information lives®

**10% Discount Coupon Code: ASTR14**