

# QUESTIONS & ANSWERS

Kill your exam at first Attempt



**Checkpoint**

# 156-915-80

*Check Point Certified Security Expert Update - R80*



# DEMO

*Find some pages taken from full version*

*Killexams 156-915-80 questions and answers are collected from Checkpoint certified professionals who recently took and pass their exam. Our 156-915-80 Exam PDF contain Organized dumps of questions and answers with references and explanations (where applicable).*

*Our target to assemble the guide is not only to pass the exam at first attempt, but really improving your knowledge about the exam topics you are dealing with.*

*Following pages are for demo purpose only. Demo pages are randomly taken from full version.*

*Full version can be different from the demo version.*

*You can request the updated Demo by contacting [support@killexams.com](mailto:support@killexams.com).*

*For Details about Full version Click <http://killexams.com/pass4sure/exam-detail/156-915-80>*

**QUESTION: 241**

Which of the following CLISH commands would you use to set the admin user's shell to bash?

- A. set user admin shell bash
- B. set user admin shell /bin/bash
- C. set user admin shell = /bin/bash
- D. set user admin /bin/bash

**Answer: B**

**QUESTION: 242**

The connection to the ClusterXL member 'A' breaks. The ClusterXL member 'A' status is now 'down'. Afterwards the switch admin set a port to ClusterXL member 'B' to 'down'. What will happen?

- A. ClusterXL member 'B' also left the cluster.
- B. ClusterXL member 'B' stays active as last member.
- C. Both ClusterXL members share load equally.
- D. ClusterXL member 'A' is asked to come back to cluster.

**Answer: B**

**QUESTION: 243**

CORRECT TEXT

Fill in the blank. To verify SecureXL statistics, you would use the command" \_\_\_\_\_

**Answer: fwaccel stats**

**QUESTION: 244**

You enable Hide NAT on the network object, 10.1.1.0 behind the Security Gateway's external interface. You browse to the Google Website from host, 10.1.1.10 successfully. You enable a log on the rule that allows 10.1.1.0 to exit the network. How many log entries do you see for that connection in SmartView Tracker?

- A. Two, one for outbound, one for inbound
- B. Only one, outbound
- C. Two, both outbound, one for the real IP connection and one for the NAT IP connection
- D. Only one, inbound

**Answer: B**

**QUESTION: 245**

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned a static IP address 10.0.0.19.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop with a static IP (10.0.0.19). He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

What should John do when he cannot access the web server from a different personal computer?

- A. John should lock and unlock his computer
- B. Investigate this as a network connectivity issue
- C. The access should be changed to authenticate the user instead of the PC
- D. John should install the Identity Awareness Agent

**Answer: C**

**QUESTION: 246**

Users with Identity Awareness Agent installed on their machines login with the domain, that information is also used to meet Identity Awareness credential requests.

- A. Key-logging
- B. ICA Certificates
- C. SecureClient
- D. Single Sign-On

**Answer:** D

**QUESTION:** 247

You cannot use SmartDashboard's User Directory features to connect to the LDAP server. What should you investigate?

- 1) Verify you have read-only permissions as administrator for the operating system.
- 2) Verify there are no restrictions blocking SmartDashboard's User Manager from connecting to the LDAP server.
- 3) Check that the login Distinguished Name configured has root permission (or at least write permission Administrative access) in the LDAP Server's access control configuration.

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

**Answer:** B

**QUESTION:** 248

Which of the following tools is used to generate a Security Gateway R80 configuration report?

- A. fw cpinfo
- B. infoCP
- C. cpinfo
- D. infoview

**Answer:** C

**QUESTION:** 249

Looking at the SYN packets in the Wireshark output, select the statement that is true

about NAT.

No. -	Time	Source	Destination	Protocol	Fire chain	Info
3	18.522170	172.21.101.201	172.21.101.3	TCP	eth0	syscomlan > ftp [SYN] Seq=0 Win
4	18.522086	172.21.101.201	10.1.1.101	TCP	eth0 I	syscomlan > ftp [SYN] Seq=0 Win
5	18.522194	172.21.101.201	10.1.1.101	TCP	eth0	eth0 o eth1 syscomlan > ftp [SYN] Seq=0 Win
6	18.522389	172.21.101.201	10.1.1.101	TCP	eth0 o eth1	syscomlan > ftp [SYN] Seq=0 Win
7	18.542114	10.1.1.101	172.21.101.201	TCP	eth0 I eth1	ftp > syscomlan [SYN, ACK] Seq=
8	18.542181	10.1.1.101	172.21.101.201	TCP	eth0	eth1 I ftp > syscomlan [SYN, ACK] Seq=
9	18.542300	10.1.1.101	172.21.101.201	TCP	eth0 o eth1	ftp > syscomlan [SYN, ACK] Seq=
10	18.542339	172.21.101.3	172.21.101.201	TCP	o eth0	eth1 ftp > syscomlan [SYN, ACK] Seq=
11	18.543211	172.21.101.201	172.21.101.3	TCP	I eth0	eth1 syscomlan > ftp [ACK] Seq=1 Ac
12	18.543259	172.21.101.201	10.1.1.101	TCP	eth0 I eth1	syscomlan > ftp [ACK] Seq=1 Ac

Frame 4 (62 bytes on wire, 60 bytes captured)  
FWI Monitor eth0 I eth1  
Internet Protocol, Src: 172.21.101.201 (172.21.101.201), Dst: 10.1.1.101 (10.1.1.101)  
Transmission Control Protocol, Src Port: syscomlan (1065), Dst Port: ftp (21), Seq: 0, Len: 0

- A. This is an example of Hide NAT.
- B. There is not enough information provided in the Wireshark capture to determine the NAT settings.
- C. This is an example of Static NAT and Translate destination on client side unchecked in Global Properties.
- D. This is an example of Static NAT and Translate destination on client side checked in Global Properties.

**Answer:** D

**QUESTION:** 250

Which of the following options is available with the GAIa cpcnfig utility on a Management Server?

- A. Export setup
- B. DHCP Server configuration
- C. GUI Clients
- D. Time & Date

**Answer:** C

**QUESTION:** 251

To qualify as an Identity Awareness enabled rule, which column MAY include an Access Role?

- A. Action
- B. Source
- C. User
- D. Track

**Answer:** B

**QUESTION:** 252

John Adams is an HR partner in the ACME organization. ACME IT wants to limit access to HR servers to designated IP addresses to minimize malware infection and unauthorized access risks. Thus, the gateway policy permits access only from John's desktop which is assigned an IP address 10.0.0.19 via DHCP.

John received a laptop and wants to access the HR Web Server from anywhere in the organization. The IT department gave the laptop a static IP address, but that limits him to operating it only from his desk. The current Rule Base contains a rule that lets John Adams access the HR Web Server from his laptop. He wants to move around the organization and continue to have access to the HR Web Server.

To make this scenario work, the IT administrator:

- 1) Enables Identity Awareness on a gateway, selects AD Query as one of the Identity Sources installs the policy.
- 2) Adds an access role object to the Firewall Rule Base that lets John Adams PC access the HR Web Server from any machine and from any location.

John plugged in his laptop to the network on a different network segment and he is not able to connect. How does he solve this problem?

- A. John should install the Identity Awareness Agent
- B. The firewall admin should install the Security Policy
- C. John should lock and unlock the computer
- D. Investigate this as a network connectivity issue

**Answer:** B

**QUESTION:** 253

The third-shift Administrator was updating Security Management Server access settings in Global Properties. He managed to lock all administrators out of their accounts. How should you unlock these accounts?

- A. Delete the file admin.lock in the Security Management Server directory \$FWDIR/tmp/.
- B. Reinstall the Security Management Server and restore using upgrade\_import.
- C. Type fwm lock\_admin -ua from the Security Management Server command line.
- D. Login to SmartDashboard as the special cpconfig\_admin user account; right-click on each administrator object and select unlock.

**Answer: C**

For More exams visit <http://killexams.com>



[KILLEXAMS.COM](http://KILLEXAMS.COM)

*Kill your exam at First Attempt....Guaranteed!*