Check Point Certified Security Administrator (CCSA)

Exam 156-215.80
Check Point Security Administrator R80.1 (CCSA)

(Demo Questions)

Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT CERTIFIED
SECURITY ADMINISTRATOR
CCSA

NO.1 Ken wants to obtain a configuration lock from other administrator on R80 Security Management Server. He can do this via WebUI or a via CLI. Which command should be use in CLI? Choose the correct answer.

A. remove database lock

B. The database feature has one command lock database override.

C. override database lock

D. The database feature has two commands: lock database override and unlock database. Both will work.

Answer: D

Explanation

Use the database feature to obtain the configuration lock. The database feature has two commands: The commands do the same thing: obtain the configuration lock from another administrator.

Description	Use the `lock database override` and `unlock database` commands to get exclusive read-write access to the database by taking write privileges to the database away from other administrators logged into the system.
Syntax	o `lock database override` o `unlock database`

NO.2 Traffic from source 192.168.1.1 is going to www.google.com. The Application Control Blade on the gateway is inspecting the traffic. Assuming acceleration is enable which path is handling the traffic?

A. Slow Path

B. Medium Path

C. Fast Path

D. Accelerated Path

Answer: A

NO.3 What are the three conflict resolution rules in the Threat Prevention Policy Layers?

A. Conflict on action, conflict on exception, and conflict on settings

B. Conflict on scope, conflict on settings, and conflict on exception

C. Conflict on settings, conflict on address, and conflict on exception

D. Conflict on action, conflict on destination, and conflict on settings

Answer: C

NO.4 Vanessa is firewall administrator in her company; her company is using Check Point firewalls on central and remote locations, which are managed centrally by R80 Security Management Server. One central location has an installed R77.30 Gateway on Open server. Remote location is using Check Point UTM-1 570 series appliance with R71. Which encryption is used in Secure Internal Communication (SIC) between central management and firewall on each location?

A. On central firewall AES128 encryption is used for SIC, on Remote firewall 3DES encryption is used for SIC.

B. On both firewalls, the same encryption is used for SIC. This is AES-GCM-256.

C. The Firewall Administrator can choose which encryption suite will be used by SIC.

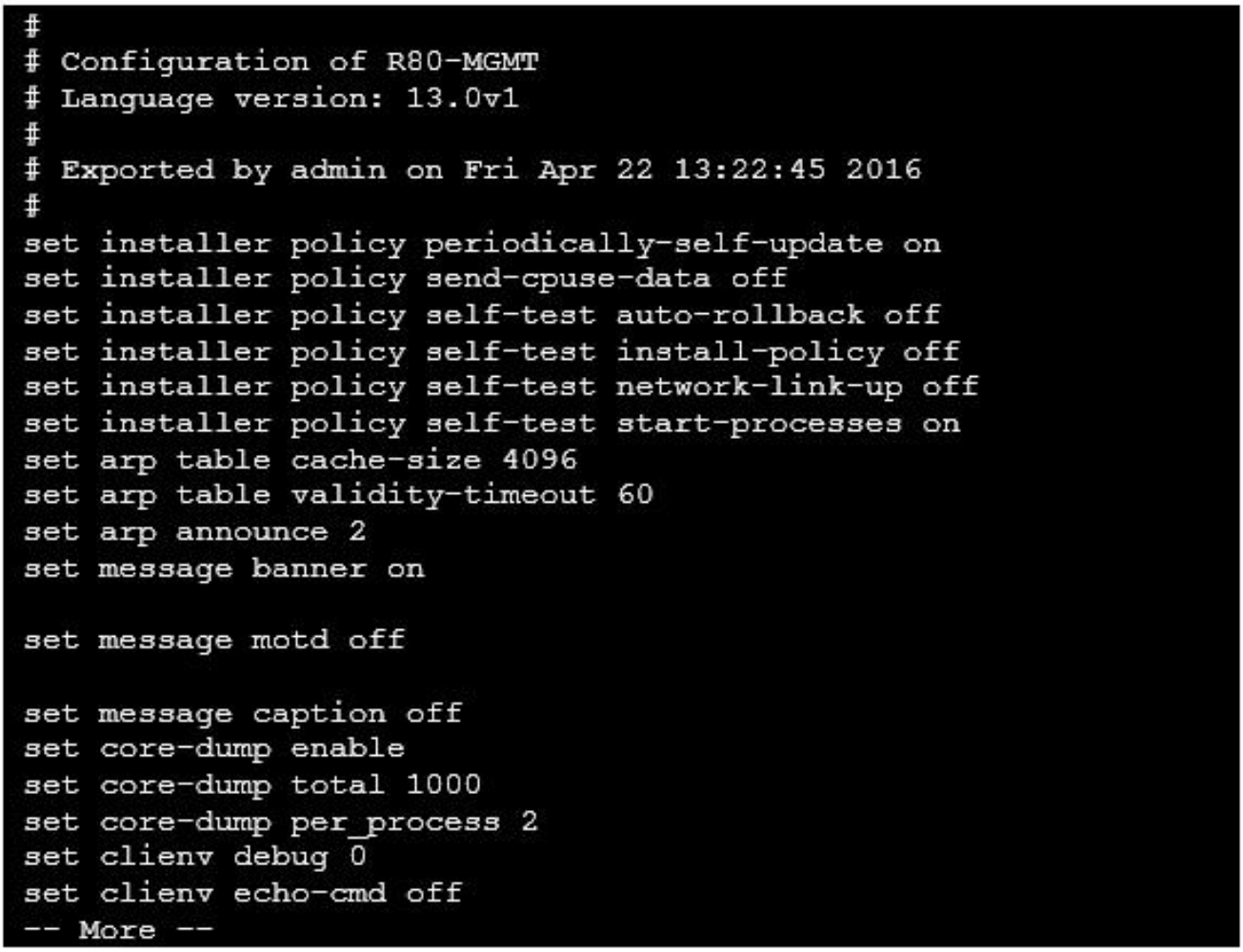
D. On central firewall AES256 encryption is used for SIC, on Remote firewall AES128 encryption is used for SIC.

Answer: A

Explanation

Gateways above R71 use AES128 for SIC. If one of the gateways is R71 or below, the gateways use 3DES.

NO.5 Look at the screenshot below. What CLISH command provides this output?



```
#
# Configuration of R80-MGMT
# Language version: 13.0v1
#
# Exported by admin on Fri Apr 22 13:22:45 2016
#
set installer policy periodically-self-update on
set installer policy send-cpuse-data off
set installer policy self-test auto-rollback off
set installer policy self-test install-policy off
set installer policy self-test network-link-up off
set installer policy self-test start-processes on
set arp table cache-size 4096
set arp table validity-timeout 60
set arp announce 2
set message banner on

set message motd off

set message caption off
set core-dump enable
set core-dump total 1000
set core-dump per_process 2
set clienv debug 0
set clienv echo-cmd off
-- More --
```

A. show configuration all

B. show confd configuration

C. show confd configuration all

D. show configuration

Answer: D

Explanation

To see the latest configuration settings, run:

```
show configuration
```

This example shows part of the configuration settings as last saved to a CLI script:

```
mem103> show configuration
#
# Configuration of mem103
# Language version: 10.0v1
#
# Exported by admin on Mon Mar 19 15:06:22 2012
#
set hostname mem103
set timezone Asia / Jerusalem
set password-controls min-password-length 6
set password-controls complexity 2
set password-controls palindrome-check true
set password-controls history-checking true
set password-controls history-length 10
set password-controls password-expiration never
set ntp active off
set router-id 6.6.6.103
set ipv6-state off
set snmp agent off
set snmp agent-version any
set snmp community public read-only
set snmp traps trap authorizationError disable
set snmp traps trap coldStart disable
set snmp traps trap configurationChange disable
```

NO.6 What are the steps to configure the HTTPS Inspection Policy?

A. Go to Manage&Settings > Blades > HTTPS Inspection > Configure in SmartDashboard

B. Go to Application&url filtering blade > Advanced > Https Inspection > Policy

C. Go to Manage&Settings > Blades > HTTPS Inspection > Policy

D. Go to Application&url filtering blade > Https Inspection > Policy

Answer: C

NO.7 As you review this Security Policy, what changes could you make to accommodate Rule 4?

No.	Hits	Name	Source	Destination	VPN	Service	Action
	Limit Access to Gateways (Rule 1)						
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
	VPN Access Rules (Rules 2-5)						
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth
5	0	Web Server	L2TP-vpn-user@Any Customers@Any	Remote-1-web-server	Any Traffic	http	accept

A. Remove the service HTTP from the column Service in Rule 4.

B. Modify the column VPN in Rule 2 to limit access to specific traffic.

C. Nothing at all

D. Modify the columns Source or Destination in Rule 4
Answer: B

NO.8 Fill in the blanks: Default port numbers for an LDAP server is _____ for standard connections and _____ SSL connections.
A. 675, 389
B. 389, 636
C. 636, 290
D. 290, 675
Answer: B
Explanation
A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports
3268, and 3269 for LDAPS.

NO.9 Which of the completed statements is NOT true? The WebUI can be used to manage user accounts and:
A. assign privileges to users.
B. edit the home directory of the user.
C. add users to your Gaia system.
D. assign user rights to their home directory in the Security Management Server
Answer: D
Explanation
Users
Use the WebUI and CLI to manage user accounts. You can:

NO.10 The SmartEvent R80 Web application for real-time event monitoring is called:
A. SmartView Monitor
B. SmartEventWeb
C. There is no Web application for SmartEvent
D. SmartView
Answer: B

NO.11 How many packets does the IKE exchange use for Phase 1 Main Mode?
A. 12
B. 1
C. 3
D. 6
Answer: D

NO.12 Which of the following is the most secure means of authentication?
A. Password
B. Certificate

C. Token
D. Pre-shared secret
Answer: B

NO.13 Which of the following Automatically Generated Rules NAT rules have the lowest implementation priority?
A. Machine Hide NAT
B. Address Range Hide NAT
C. Network Hide NAT
D. Machine Static NAT
Answer: B C
Explanation
SmartDashboard organizes the automatic NAT rules in this order:

NO.14 Vanessa is expecting a very important Security Report. The Document should be sent as an attachment via e-mail. An e-mail with Security_report.pdf file was delivered to her e-mail inbox. When she opened the PDF file, she noticed that the file is basically empty and only few lines of text are in it. The report is missing some graphs, tables and links. Which component of SandBlast protection is her company using on a Gateway?
A. SandBlast Threat Emulation
B. SandBlast Agent
C. Check Point Protect
D. SandBlast Threat Extraction
Answer: D

NO.15 You are conducting a security audit. While reviewing configuration files and logs, you notice logs accepting POP3 traffic, but you do not see a rule allowing POP3 traffic in the Rule Base. Which of the following is the most likely cause?
A. The POP3 rule is disabled.
B. POP3 is accepted in Global Properties.
C. The POP3 rule is hidden.
D. POP3 is one of 3 services (POP3, IMAP, and SMTP) accepted by the default mail object in R77.
Answer: C

NO.16 If there is an Accept Implied Policy set to "First", what is the reason Jorge cannot see any logs?
A. Log Implied Rule was not selected on Global Properties.
B. Log Implied Rule was not set correctly on the track column on the rules base.
C. Track log column is set to none.
D. Track log column is set to Log instead of Full Log.
Answer: A
Explanation
Implied Rules are configured only on Global Properties.

NO.17 Choose the correct statement regarding Implicit Rules.
A. To edit the Implicit rules you go to: Launch Button > Policy > Global Properties > Firewall.
B. Implied rules are fixed rules that you cannot change.
C. You can directly edit the Implicit rules by double-clicking on a specific Implicit rule.
D. You can edit the Implicit rules but only if requested by Check Point support personnel.
Answer: A

NO.18 You noticed that CPU cores on the Security Gateway are usually 100% utilized and many packets were dropped. You don't have a budget to perform a hardware upgrade at this time. To optimize drops you decide to use Priority Queues and fully enable Dynamic Dispatcher. How can you enable them?
A. fw ctl multik dynamic_dispatching on
B. fw ctl multik dynamic_dispatching set_mode 9
C. fw ctl multik set_mode 9
D. fw ctl miltik pq enable
Answer: C

NO.19 Which of the following are types of VPN communicates?
A. Pentagon, star, and combination
B. Star, octagon, and combination
C. Combined and star
D. Meshed, star, and combination
Answer: D

NO.20 While enabling the Identity Awareness blade the Identity Awareness wizard does not automatically detect the windows domain. Why does it not detect the windows domain?
A. Security Gateways is not part of the Domain
B. SmartConsole machine is not part of the domain
C. SMS is not part of the domain
D. Identity Awareness is not enabled on Global properties
Answer: B
Explanation
To enable Identity Awareness:
The Identity Awareness Configuration wizard opens.
See Choosing Identity Sources.
Note - When you enable Browser-Based Authentication on a Security Gateway that is on an IP Series appliance, make sure to set the Voyager management application port to a port other than 443 or 80.
The Integration With Active Directory window opens.
When SmartDashboard is part of the domain, SmartDashboard suggests this domain automatically. If you select this domain, the system creates an LDAP Account Unit with all of the domain controllers in the organization's Active Directory.

NO.21 Jennifer McHanry is CEO of ACME. She recently bought her own personal iPad. She wants use her iPad to access the internal Finance Web server. Because the iPad is not a member of the Active

Directory domain, she cannot identify seamlessly with AD Query. However, she can enter her AD credentials in the Captive Portal and then get the same access as on her office computer. Her access to resources is based on rules in the R77 Firewall Rule Base.
To make this scenario work, the IT administrator must:
1) Enable Identity Awareness on a gateway and select Captive Portal as one of the Identity Sources.
2) In the Portal Settings window in the User Access section, make sure that Name and password login is selected.
3) Create a new rule in the Firewall Rule Base to let Jennifer McHanry access network destinations. Select accept as the Action.
4) Install policy.
Ms McHanry tries to access the resource but is unable. What should she do?

A. Have the security administrator select the Action field of the Firewall Rule "Redirect HTTP connections to an authentication (captive) portal".

B. Have the security administrator reboot the firewall.

C. Have the security administrator select Any for the Machines tab in the appropriate Access Role.

D. Install the Identity Awareness agent on her iPad.

Answer: A

NO.22 Which of the following blades is NOT subscription-based and therefore does not have to be renewed on a regular basis?

A. Application Control

B. Threat Emulation

C. Anti-Virus

D. Advanced Networking Blade

Answer: B

NO.23 In which scenario is it a valid option to transfer a license from one hardware device to another?

A. From a 4400 Appliance to an HP Open Server

B. From an IBM Open Server to an HP Open Server

C. From an 4400 Appliance to a 2200 Appliance

D. From an IBM Open Server to a 2200 Appliance

Answer: B

NO.24 Fill in the blank: To create policy for traffic to or from a particular location, use the _____.

A. DLP shared policy

B. Geo policy shared policy

C. Mobile Access software blade

D. HTTPS inspection

Answer: B

Explanation
Shared Policies
The Shared Policies section in the Security Policies shows the policies that are not in a Policy package.

They are shared between all Policy packages.
Shared policies are installed with the Access Control Policy.
Software Blade
Description
Mobile Access
Launch Mobile Access policy in a SmartConsole. Configure how your remote users access internal resources, such as their email accounts, when they are mobile.
DLP
Launch Data Loss Prevention policy in a SmartConsole. Configure advanced tools to automatically identify data that must not go outside the network, to block the leak, and to educate users.
Geo Policy
Create a policy for traffic to or from specific geographical or political locations.

NO.25 Fill in the blanks: There are _____ types of software containers _____.
A. Three; security management, Security Gateway, and endpoint security
B. Three; Security gateway, endpoint security, and gateway management
C. Two; security management and endpoint security
D. Two; endpoint security and Security Gateway
Answer: A
Explanation
There are three types of Software Containers: Security Management, Security Gateway, and Endpoint Security.

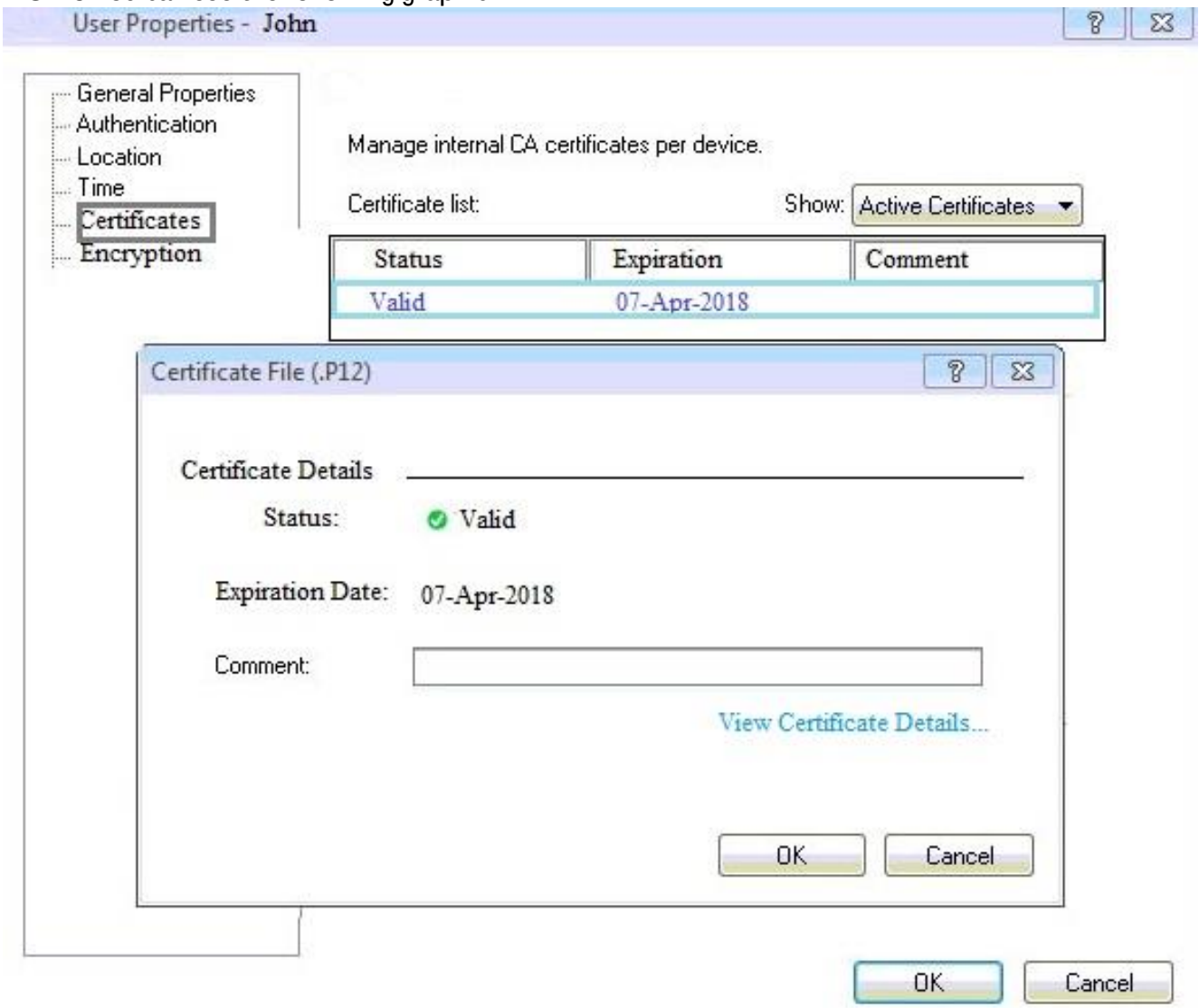
NO.26 Which icon indicates that read/write access is enabled?
A. Pencil
B. Padlock
C. Book
D. Eyeglasses
Answer: A

NO.27 During the Check Point Stateful Inspection Process, for packets that do not pass Firewall Kernel Inspection and are rejected by the rule definition, packets are:
A. Dropped without sending a negative acknowledgment
B. Dropped without logs and without sending a negative acknowledgment
C. Dropped with negative acknowledgment
D. Dropped with logs and without sending a negative acknowledgment
Answer: D

NO.28 You are the Check Point administrator for Alpha Corp with an R80 Check Point estate. You have received a call by one of the management users stating that they are unable to browse the Internet with their new tablet connected to the company Wireless. The Wireless system goes through the Check Point Gateway. How do you review the logs to see what the problem may be?
A. Open SmartLog and connect remotely to the IP of the wireless controller
B. Open SmartView Tracker and filter the logs for the IP address of the tablet

C. Open SmartView Tracker and check all the IP logs for the tablet
D. Open SmartLog and query for the IP address of the Manager's tablet
Answer: B

NO.29 You can see the following graphic:



What is presented on it?
A. Properties of personal .p12 certificate file issued for user John.
B. Shared secret properties of John's password.
C. VPN certificate properties of the John's gateway.
D. Expired .p12 certificate properties for user John.
Answer: A