

Vendor: Check Point

Exam Code: 156-215.71

Exam Name: Check Point Certified Security Administrator R71

Version: Demo

### **QUESTION 1**

You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? i.e. the command cprestart is not sufficient.

A. 3 only

- B. 1, 2, 3, 4, and 5
- C. 2, 3 only
- D. 3, 4, and 5 only

Answer: C

### **QUESTION 2**

Of the following, what parameters will not be preserved when using Database Revision Control?

Simplified mode Rule Bases
 Traditional mode Rule Bases
 Secure Platform WebUI Users
 SIC certificates
 SmartView Tracker audit logs
 SmartView Tracker traffic logs
 Implied Rules
 IPS Profiles
 Blocked connections
 Manual NAT rules
 VPN communities
 Gateway route table
 Gateway licenses

A. 3, 4, 5, 6, 9, 12, 13
B. 5, 6, 9, 12, 13
C. 1, 2, 8, 10, 11
D. 2, 4, 7, 10, 11

Answer: B

#### **QUESTION 3**

To reduce the information given to you in SmartView Tracker, what can you do to find information about data being sent between pcosaka and pctokyo?

- A. Double-click an entry representing a connection between both endpoints.
- B. Press CTRL+F in order to open the find dialog, and then search the corresponding IP addresses.
- C. Apply a source filter by adding both endpoint IP addresses with the equal option set.
- D. Use a regular expression to filter out relevant logging entries.

### Answer: C

### **QUESTION 4**

A third-shift Security Administrator configured and installed a new Security Policy early this morning. When you arrive, he tells you that he has been receiving complaints that Internet access is very slow. You suspect the Security Gateway virtual memory might be the problem. Which

SmartConsole component would you use to verify this?

- A. SmartView Tracker
- B. SmartView Monitor
- C. This information can only be viewed with fw ctl pstat command from the CLI.
- D. Eventia Analyzer

### Answer: B

# **QUESTION 5**

From the output below, where is the fingerprint generated?

SmartL	Dashboard <sup>®</sup> Check Poin
R71	
This is the first ti	me you are contacting this server.
Server:	192 168 25 101 - 192 168 25 101
Eingerprint:	DEL YES HIRE KANE ATE BOOK OW NED COED FROM GO HILL
	sure that no one is impersonating your
To be absolutely management, co on the server, to	ompare the Fingerprint in the Configuration Tool

- A. SmartUpdate
- B. Security Management Server
- C. SmartDashboard
- D. SmartConsole

#### Answer: B

### **QUESTION 6**

When troubleshooting NAT entries in SmartView Tracker, which column do we need to check to view the new source IP when using NAT?

- A. XlateSrc
- B. XlateSPort
- C. XlateDst
- D. XlateDPort

#### Answer: A

### **QUESTION 7**

When troubleshooting NAT entries in SmartView Tracker, which column do we need to check to view the NAT'd source port when using source NAT?

- A. XlateDst
- B. XlateDPort
- C. XlateSPort
- D. XlateSrc

### Answer: C

### **QUESTION 8**

Which Client Authentication sign-on method requires the user to first authenticate via the User Authentication mechanism when logging in to a remote server with Telnet?

- A. Standard Sign On
- B. Manual Sign On
- C. Agent Automatic Sign On
- D. Partially Automatic Sign On

### Answer: D

#### **QUESTION 9**

When selecting an authentication scheme for a user, which scheme would you use if you only want the password to be stored locally?

General Properties Groups	Authentication		
Authentication Location			-
Time Certificates	Authentication Scheme: Settings	Undefined Undefined	~
Encryption		Securit Check Point Password OS Password RADIUS TACACS	
		No Specific Settings	
		OK Cancel	Help

(The password is not stored at a third party component.)

- A. Check Point Password
- B. TACACS
- C. SecurID
- D. OS Password

Answer: A

### **QUESTION 10**

Phase 2 uses \_\_\_\_\_\_, if not using Perfect Forward Secrecy.

- A. Symmetric
- B. Conditional
- C. Sequential
- D. Asymmetric

### Answer: A

# **QUESTION 11**

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

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

### Answer: B

# **QUESTION 12**

You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

- A. Add a "temporary" rule using SmartDashboard and select hide rule.
- B. Create a Suspicious Activity Rule in SmartView Monitor
- C. Use dbedit to script the addition of a rule directly into the Rule Bases\_5\_0. fws configuration file.
- D. Select block intruder from the tools menu in SmartView Tracker.

### Answer: B

### **QUESTION 13**

The Check Point Security Gateway's virtual machine (kernel) exists between which two layers of the OSI model?

- A. Session and Network layers
- B. Application and Presentation layers
- C. Physical and Data link layers
- D. Network and Data link layers

### Answer: D

### **QUESTION 14**

Phase 1 uses\_\_\_\_\_

.

- A. Conditional
- B. Sequential
- C. Asymmetric
- D. Symmetric

#### Answer: C

# **QUESTION 15**

What is a possible reason for the IKE failure shown in this screenshot?

Product	VPN-1 Power/UTM	Action	Om Key Install
Date	21Jul2009	Rule	
Time	15:13:03	Current Rule Number	
Number	6503	Rule Name	
Туре	Log	User	
Origin	fwsingapore	P.	
		Encryption Scheme	IKE IKE
Source	fwfrankfurt (172.30.110.1)	IKE Initiator Cookie	3328abc431cf19f6
Destination	fwsingapore (172.28.108.1)	IKE Responder	2917/df5a8c831e3
Service	+	Cookie	
Protocol		VPN Peer Gateway	fwfrankfurt (172.30.110.1)
Interface	\Xi daemon	Subproduct	O VPN
Source Port		VPN Feature	IKE
		Information	IKE: Phase1 Received
			Notification from Peer:
Policy Name			payload malformed
Policy Date	1 and		
Policy Management	S ###		

- A. Mismatch in VPN Domains.
- B. Mismatch in Diffie-Hellman group.
- C. Mismatch in encryption schemes.
- D. Mismatch in preshared secrets.

### Answer: D

### **QUESTION 16**

Which of the following uses the same key to decrypt as it does to encrypt?

- A. Asymmetric encryption
- B. Symmetric encryption
- C. Certificate-based encryption
- D. Dynamic encryption

### Answer: A

## **QUESTION 17**

When configuring the network interfaces of a checkpoint Gateway, the direction can be defined as Internal or external. What is meaning of interface leading to DMZ?

neral Topology	Member Network	QoS	Multicast Re	strictions
opology				
External (leads	out to the internet)			
Internal (leads t	o the local network	:)		
IP Addresses	behind this interfa	ce:		
Not Defin	ed			
Network	defined by the inter	face IP an	d Net Mask	
Specific:		>		New
V Interface	leads to DMZ	)	6	
	C. N. C. C. C.			
nti-Spoofing		201 March 11 (201		
nti-Spoofing ] <u>P</u> erform Anti-Sp	coling based on in	terface to;	book	
Perform Anti-Sp	oofing based on in ick packets from:	terface to:	, hoodl	New
Perform Anti-Sp		Co Log		
Perform Anti-Sp	ick packets from:			
Perform Anti-Sp	ick packets from:			

- A. It defines the DMZ Interface since this information is necessary for Content Control.
- B. Using restricted Gateways, this option automatically turns off the counting of IP Addresses originating from this interface
- C. When selecting this option. Ann-Spoofing is configured automatically to this net.
- D. Activating this option automatically turns this interface to External

# Answer: A

### **QUESTION 18**

For which service is it NOT possible to configure user authentication?

# A. HTTPS

- B. FTP
- C. SSH
- D. Telnet

Answer: C

# **QUESTION 19**

What can NOT be selected for VPN tunnel sharing?

- A. One tunnel per subnet pair
- B. One tunnel per Gateway pair
- C. One tunnel per pair of hosts
- D. One tunnel per VPN domain pair

# Answer: D

# **QUESTION 20**

You run cpconfig to reset SIC on the Security Gateway. After the SIC reset operation is complete, the policy that will be installed is the

- A. Last policy that was installed
- B. Default filter
- C. Standard policy
- D. Initial policy

Answer: D