TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **156-915-70**

Title : Check Point Certified Security Expert CCSE-R70-Update

Version : Demo

1.What is the benefit to running Eventia Analyzer in Learning Mode?
A. There is no Eventia Analyzer Learning Mode
B. To run Eventia Analyzer, with a step-by-step online configuration guide for training/setup purpose
C. To run Eventia Analyzer with preloaded sample data in a test environment
D. To generate a report with system Event Policy modification suggestions
Answer: D

2.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: B

3.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

4.What is the maximum number of cores supported by CoreXL?
A. 6
B. 8
C. 4
D. 12
Answer: B

5.Which of the following commands will stop acceleration on a Security Gateway running on Secure Platform?
A. splat_accel off
B. fwacceX off
C. perf_pack off
D. fwaceel off
Answer: D

6.Which of the following is not accelerated by SecureXL?
A. FTP
B. HTTPS
C. Telnet
D. SSH
Answer: A

7.You want VPN traffic to match packets from internal interfaces- You also want the traffic to exit the Security Gateway bound for all site-to-site VPN Communities, including Remote Access Communities. How should you configure the VPN match rule?
A. Communities > communities
B. Internal_clear > External_Clear
C. Internal_clear > All_GwTogw
D. Internal_clear > All_communities
Answer: D

8.The London office just upgraded their DNS Gateway needs with the new settings. What would be the best way for Henry to change the DNS settings for the London's Gateway?
A. Edit the Canada profile
B. Edit the gateways DNS settings from the edit gateway, then selecting the DNS tab
C. DNS settings for that gateway cannot be changed
D. Edit the Europe profile
Answer: B

9.What are the SmartProvisioning Policy Status indicators?
A. OK, Down, Up, Synchronized
B. OK. Waiting, Out of Sync, Not Installed, Not communicating
C. OK, Unknown, Not Installed, May be out of date
D. OK, Waiting, Unknown, Not Installed, Not Updated, May be out of date
Answer: D

10.Which specific R70 GUI would you use to view the length of time a TCP connection was open?
A. SmartView Tracker
B. SmartView Status
C. SmartView Monitor
D. Eventia Reporter
Answer: C

11.You have selected the event "port scan from internal network in Eventia Analyzer", to detect an event when 30 ports have occurred when 60 seconds. You want to detect two ports scans from a host within 10 seconds of each other. How would you accomplish this?
A. You cannot set Eventia Analyzer to detect two port scans within 10 seconds of each other.
B. Select the two port-scan detections as a new event.
C. Select the two port-scan detections as a sub event.
D. Select the two port-scan detections as an exception.
Answer: D

12.When checkpoint product is used to create and save changes to a Log consolidation policy?
A. Security Management Server
B. Eventia Reporter Client
C. SmartDashboard Log Consolidator

D. Eventia Reporter Server
Answer: D

13.Reporter reports can be used to analyze data from a penetration-testing regimen in all of the following examples, EXCEPT
A. Possible worm/malware activity.
B. Tracking attempted port scans.
C. Analyzing traffic patterns against public resources.
D. Analyzing access attempts via social-engineering.
Answer: D

14.Laura notices the Microsoft Visual Basic kill Bits protection is sent to inactive. She wants to set the micro soft Visual Basic Kill bits protection and all other low performance impact protection to prevent. She asks her manager for approval and he stated she can turn these on. But he Laura to make sure no high performance impact protections are limited on while changing this setting.
Using the output below, how would Laura change the default-protection on performance impact protections classified as low from inactive to prevent while still meeting her other criteria?
A. Go to profiles > Default_protection and unlock “Do not activate protections with performance impact to medium or above”
B. Go to profiles > Default_protection and select “Do not activate protections with performance impact to low or above”
C. Go to profiles > Default_protection and select “Do not activate protections with performance impact to medium or above”
D. Go to profiles > Default_protection and unlock “Do not activate protections with performance impact to high or above”
Answer: C

15.John is the MultiCorp Security Administrator. If he suggests a change in the firewall configuration, he must submit his proposal to David, a Security manager. One day David is out of the office and john submits his proposal to peter, surprisingly, Peter is not able to approve the proposal the system does not permit him to do so (See figure below)
Next day David is back and he can carry out this operation.
Both the David and peter have accounts as administrators in the Security management Server and both have the read/write all permission. What is the reason for the difference? Choose the best answer.
A. There were some hardware/software issues at the Security management Server on the first day.
B. Peter was not log on to system for a long time.
C. The attribute manage administrators was not assigned to peter.
D. The specific SmartWorkflow read/write permissions were assigned to David only.
Answer: D

16.Which of the following is a supported deployment for Connectra?
A. IPSO 4.9 build 88
B. VMWare ESX
C. Solaris 10

D. Windows server 2007
Answer: B

17.From the following output of cphaprob state, which ClusterXL mode is this?
A. New mode
B. Multicast mode
C. Legacy mode
D. Unicast mode
Answer: D

18.Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?
A. VTIs must be assigned a proxy interface.
B. VTIs can only be physical, not loopback.
C. Local IP addresses are not configured, remote IP addresses are configured.
D. VTIs are only supported on Secure Platform.
Answer: C

19.Which type of routing relies on a VPN Tunnel interface (VT1) to route traffic?
A. Subnet-based VPN
B. Route-based VPN
C. Host-based VPN
D. Domain-based VPN
Answer: B

20.What is a task of the IPS Event Analysis Server?
A. Assign a severity level to an event.
B. Display the received events.
C. Forward what is known as an event to the IPS Event Analysis server
D. Analyze each IPS log entry as it enters the Log server.
Answer: D

21.Using IPS, how do you notify the Security Administrator that malware is scanning specific ports?
By enabling:
A. Malware Scan protection
B. Sweep Scan protection
C. Host Port Scan
D. Malicious Code Protector
Answer: C

22.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

23.Which Security Servers can perform authentication tasks, but CANNOT perform content security tasks?
A. RLOGIN
B. FTP
C. HTTPS
D. HTTP
Answer: A

24.What is the purpose of the pre-defined exclusions Included with Eventia Analyzer and IPS Event Analysis R7P?
A. To give samples of how to write your own exclusion.
B. As a base for starling and building exclusions
C. To allow Eventia Analyzer and IPS Event Analysis R70 to function property with all other R70 release devices
D. To avoid incorrect event generation by the default IPS event definition, a scenario that may occur in deployments that include Security Gateways of versions prior to R70
Answer: D

25.You are trying to configure Directional VPN Rule Match in the Rule Base. But the match column does not have the option to see the directional match. You see the following window. What must you enable to see the Directional match?
A. VPN Directional Match on the Gateway object's VPN tab
B. Advanced Routing on each Security Gateway
C. VPN Directional Match on the VPN advanced Window, m Global Properties
D. Directional_match (True) in the objects_5_0 file on Security management Server
Answer: C

26.You believe Phase 2 negotiations are failing while you are attempting to configure a site-to-site VPN with one of your firm's business partners. Which SmartConsole application should you use to confirm your suspicions?
A. SmartDashboard
B. SmartView Tracker
C. SmartUpdate
D. SmartView Status
Answer: B

27.The ‘We-Make-Widgets’ company has purchased twenty UTM-1 Edge appliances for their remote offices. Kim decides the best way to manage those appliances is to use SmartProvisioning and create a profile they can all use. List the order of steps Kim would go through to add the Dallas Edge appliance to the remote Office profile Using the output below.
A. 6, 1, 3, 4, 5, 2
B. 4, 1, 3, 6, 5, 2

C. 6, 3, 1, 4, 5, 2
D. 4, 3, 1, 6, 5, 2
Answer: B

28.You are Connectra administrator. Your users complain that their outlook Web Access is running extremely slowly, and their overall browsing experience configures to worsen. You suspect it could be a logging problem. Which of the following log file does CheckPoint recommended you purge?
A. Httpd*.log
B. Event_ws.log
C. Mod_ws_owd.log
D. Alert_owd.log
Answer: A

29.With Eventia Analyzer, what is the analyzer Server's function?
A. Generate a threat analysis report from the Analyzer database.
B. Analyze log entries, looking for Event Policy patterns.
C. Displays received threats and tune the Events Policy.
D. Assign seventy levels to events.
Answer: B

30.You have pushed a policy to your firewall and you are not able to access the firewall. What command will allow you to remove the current policy from the machine?
A. fw purge policy
B. fw fetch policy
C. fw purge active
D. fw unload local
Answer: D