Vendor: Check Point

Exam Code: 156-915.71

Exam Name: Check Point Certified Security Expert update blade

Version: DEMO

1.Which SmartEvent, what is the Correlation Unit's function?
A. Invoke and define automatic reactions and add events to the database
B. Assign seventy levels to events
C. Display received threats and tune the Events Policy
D. Analyze log entries, looking for Event Policy patterns
Answer: D

2.How do you verify the Check Pant kernel running on a firewall.?
A. fw ctrl get kernel
B. fw ctrl pstat
C. fwkernel
D. fwver -k
Answer: D

3.After repairing a SmartWorkflow session:
A. The session moves to status Repaired and a new session can be started
B. The session moves to status Awaiting Repair and must be resubmitted
C. The session is continued with status Not approved and a new session must be started
D. The session is discarded and a new session is automatically started
Answer: B

4.TotallyCoolSecuirty Company has a large security staff. Bob configured a new IPS Chicago_Profile for fw-Chicagousing Detect mode. After reviewing Matt noticed that fw-Chicagois not detecting any of the IPS protections that Bob had previously setup. Analyze the output below and determine how Mattcorrectsthe problem.
A. Matt should assign the fw-ChicagoSecurity Gateway to theChicago_Profile.
B. Matt should theChicago_Profile to useProtect mode because Detect mode
C. Matt should re-create theChicago_Profile and select Activeprotections manually instead of per theIPSPolicy.
D. Mattshouldactivatethe Chicago_Profileasitis currently notactivated.
Answer: A

5.Which Remote Desktop protocols are supported natively in SSL VPN?
A. Microsoft RDP only
B. AT&T VNC and Microsoft RDP
C. Citrix ICA and Microsoft RDP
D. AT&T VNC, Citrix ICA and Microsoft RDP
Answer: D

6.To force clients to use integritySecurity Workspace when accessing sensitive applications, the Administrator can configure Connectra:
A. Via protection levels
B. To implement integrity Clientless Security

C. To force the user to re-authenticate at login
D. Without a special setting. Secure Workspace is automatically configured.
Answer: A

7.The default port for browser access to the Management Portal is
A. 4433
B. 4343
C. 8080
D. 443
Answer: A

8.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

9.YoujustupgradedtoR71 and are using the IPS Software Blade You want toenable all critical protections while keeping the rate of false positively verylow.How can you achieve this?
A. The new IPS system is basedon policies, but it has no abilitytocalculate or change the confidence level, so it always has a high rate of falsepositives.
B. This can t be achieved; activating any IPS system always causes ahigh rate of false positives.
C. The new IPS system is based on policies and gives you the abilitytoactivate all checks with critical severity and a high confidence level.
D. As in SmartDefense,this can be achieved by activating all the criticalchecks manually.
Answer: C

10.Refer to the network topology below. You have IPS Software Blades active on the Security Gateways sglondon, sgla, andsgny, but still experience attacks on the Web server in the New York DMZ. How is this possible?
A. AH of these options are possible.
B. The attacker may have used a bunch of evasion techniques likeusing escape sequence instead of cleartext commands.It is also possible that thereare entry points not shown in the network layout, like rogue access points.
C. Since other Gateways do not have IPS activated, attacks may originate from their network without anyone noticing.
D. An IPS may combine different detection technologies, but is dependent on regular signature updates and well-turned anomaly algorithms.Even if this is accomplished, notechnology can offer 100 % protection.
Answer: C

11.Which of the following is NOT an Smartevent event-triggered Automatic Reaction?

A. Mail
B. Block Access
C. External Script
D. SNMP Trap
Answer: B

12.Your company has the requirement that SmartEvent reports should show a detailed and accurate view of network activity but also performance should be guaranteed. Which actions should be taken to achieve that?
A. (i), (ii) and (iv)
B. (i), (iii), (iv)
C. (ii) and (iv)
D. (i) and (ii)
Answer: C

13.What SmartConsole application allows you to change the Log Consolidation Policy?
A. SmartReporter
B. SmartUpdate
C. SmartEvent Server
D. Smart Dashboard
Answer: A

14.In configure a client to property log in to the user portal using a certificate, the Administrator MUST:
A. Create aninternal userin the admin portal.
B. Install an R71 internal Certificate Authority certificate.
C. Create a client certificate fromSmart Dashboard
D. Store the clientcertificate on the SSL VPN Gateway
Answer: C

15.What process manages the dynamic routing protocols (ospp, RIP, etc) on SecurelPlatform Pro?
A. gated
B. arouted
C. routerd
D. There s no separate process, but the Linux default router can take care of that.
Answer: A

16.To change the default port of the Management Portal,
A. Editthe masters.conffileon the Portal server.
B. Modify the file cp_httpd_admin.conf.
C. Run sysconfig and change the management interface
D. Re-initializeSIC.

Answer: C

17.Where do Gateways managed by SmartProvisioning fetch their assigned profiles?
A. The Smartview Monitor
B. The standalone SmartProvisioning server
C. The Security Management server or CMA
D. They are fetched locally from the individual device
Answer: C

18.When synchronizing clusters, which of the following statements is NOT true?
A. Client Auth or Session Auth connections through a cluster member will be lost if the cluster member fails.
B. The stare of connection using resources is maintained by a Security Server, so there connections cannot be synchronized.
C. Only cluster members running on me same OS platform can be synchronized.
D. In the case of a failover, accounting information on the failed member may be lost despite a properly working synchronization.
Answer: D

19.What command will allow you to disable sync on a cluster firewall member?
A. fw ctl setaync 0
B. fw ctl syncsatat stop
C. fw ctl syncstat off
D. fw ctl setsync off
Answer: D

20.By default, a standby Security Management Server is automatically synchronized by an active Security Management Server, when:
A. The Security Policy is saved.
B. The Security Policy is installed.
C. The user database is installed.
D. The standby Security Management Server starts for the first time.
Answer: A

21.A customer is calling saying one member's status is Down.What will you check?
A. cphaprob list (verify what critical device is down)
B. Fw ctl debug m cluster + forward(forwarding layer debug)
C. tcpdump/snoop (CCP traffic)
D. fw ctlpstat (check sync)
Answer: A

22.You have a High Availability ClusterXL configuration.Machines arenot synchronizer. What happens to connections on failover?

A. It is not possible to configure High Availabilitythat is not synchronized.
B. B. Old connections are lost but can be reestablished.
C. Connection cannot be established until cluster members are fully synchronized.
D. Old connections are lost but are automatically recovered whenever the failed machine recovers.
Answer: B

23.When using ClusterXl in load sharing, what method is used be default?
A. IPs, SPIs
B. IPs, Ports, SPIs
C. IPs
D. IPs, Ports
Answer: C

24.John isconfiguring anew R17 Gateway cluster but he cannot configurethecluster asThird Party IP Clusteringin Gateway Cluster Properties:
What s happening?
A. Johnis not using thirdparty hardware asIP Clustering ispart of Check Point sIPAppliance.
B. Third Party Clustering is not available for R71 Security Gateways.
C. ClusterXLneeds to be unsetected to permit 3nd party clustering configuration.
D. John has an invalid ClusterXL license
Answer: C

25.A customer calls saying that a load-sharing cluster shows drops with the error First packet is notSYN.Completethe followingsentence. I will recommend:
A. Change the load on each member.
B. configuring flush and ack
C. turning off SDF (Sticky Decision Function)
D. turning on SDF (Sticky Decision Function)
Answer: D

26.Which at the followingcommands showsfull synchronization status?
A. cphaprob-ilist.
B. fw ctliflist
C. Fw hastat
D. cphaprob aif
Answer: A

27.If Victor wanted to edit new Signature Protections, what tab would he need to access inSmart Dashboard?
A. QoS Tab
B. SmartDefense Tab
C. IPSec VPN Tab

D. IPS Tab
Answer: D

28.Due to some recent performance issues, you are asked to add additional processors to your firewall. If you already have CoreXL enabled, how are you able to increase Kernel instances?
A. Kernel instances are automatically added after process installed and no additional configuration is needed.
B. In SmartUpdate, right-click on Firewall Object and choose Add Kernel instances.
C. Once CoreXL is installed you cannot enable additional Kernel instances without reinstalling R71.
D. Use cpconfig to reconfigure CoreXL.
Answer: D

29.Which of the following is the default port few Management Portal?
A. 4434
B. 443
C. 444
D. 4433
Answer: D

30.Whichof theft flowing is TRUE concerning unnumberedVPNTunnelInterfaces (VTIs)?
A. VTTs cannot be assigned a proxy interface
B. Local IP addresses are not configured, remoteIPaddresses are configured
C. VTIs can only be physical, not loopback
D. VTIs are only supported on the IPSO Operating System
Answer: B