Check Point Set-1

1. Before Security Gateways can exchange encryption keys and build VPN tunnels, they first need

to authenticate to each other. What are the types of Ans. Certificates 2. Which command line interface utility allows the administrator to verify the name and

timestamp of the Security Policy currently instructed. Ans. Fw stat 3. Which tool is used to control VPN tunnels?

Ans. vpn tu 4. How to check the mds server (provider -1) service status

Ans. Mdsstat 5. Secure communication from CMAs to the Security Gateways user which type of encryption?

Ans. 128-bit SSL encryption 6. What are the security measures are taken to ensure the safety of SIC?

**Ans. 3DES for encryption 7. What are the components are available in the security rule.**

1. Source IP 8. 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 Ans. Initial policy 9. Your company's Security Policy forces users to authenticate to the Gateway explicitly, before

they can use any services. The Gateway does not allow Telnet service to itself from any location. How would you set up the authentication method With. Ans. Client Authentication rule using the manual sign-on method, using HTTP on port 900 10. Which of the applications in check point technology can be used to configure security objects?

1. Smart Dashboard 2. Smartview Monitor 3. Smartview Tracker 4. Smart Event Manager 11. Commands to configure the address resolution protocol (ARP).

12. Which of the following can be found in cpinfo from an enforcement point?

Ans. The complete file objects\_5\_0. C 13. Where are automatic NAT rules added to the Rule Base?

**Ans. Last 14. All Check point products come with a 15-day trial-period license. How many CMAs can be**

managed by an MDS Manager running with only. Ans. 500 15. During which step in the installation process is it necessary to note the fingerprint for first-time

verification? Ans. When configuring the Security Management Server using cpconfig 16. The revert operation allows you to revert to a previously saved version. Once you initiate the

revert operation, the selected version overwrites the current policy. The one type of information that is not overwritten, is Ans. Certificate Authority (CA) data 17. Which R77 SmartConsole tool would you use to verify the installed Security Policy name on a

Security Gateway?

Ans. SmartView Tracker 18. which nat method allows you to external traffic to access internal resources.

Ans. Static 19. Which column in the Rule Base is used to define authentication parameters?

Ans. Action 20. The most recommended and manageable method for authentication among gateways and

remote clients is: Ans. Digital certificates

**Check Point Set-2**

21. Which services are supported by VPN-1/Firewall-1 User Authentication?

**Ans. Telnet, FTP, RLOGIN, HTTP, HTTPS**

22. If you are experiencing LDAP issues, which of the following should you check? Ans. Connectivity between the R75 Gateway and LDAP server

23. Which of the below is the MOST correct process to reset SIC from SmartDashboard?

**Ans. Click the Communication button for the firewall object, then click Reset. Run cpconfig and type a new activation key. 24. what method used to ensures that policy package is not mistakenly installed on any appropriate**

target Ans. Installation target 25. David wants to manage hundreds of gateways using a central management tool. What tool

would David use to accomplish his goal? Ans. SmartBlade 26. how to fix the issue for firewall fwx\_cache error

Ans. add the table size 27. The most recommended and manageable method for authentication among gateways and

remote clients is: Ans. Digital certificates 28. SmartView Tracker logs the following Security Administrator activities, EXCEPT

Ans. Tracking SLA compliance. 29. How do you define a service object for a TCP port range?

Ans. Manage Services, New TCP, Provide name and define Port: x-y 30. what is the advantages of client authentication

Ans. Unlimited number of connections 31. how do you check the cluster status on the checkpoint firewall

Ans. Cphaprob stat 32. If a Security Gateway enforces three protections, LDAP Injection, Malicious Code Protector, and

Header Rejection, which Check Point license is required in SmartUpdate? Ans. IPS 33. Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces (VTIs)?

Ans. Local IP addresses are not configured, remote IP addresses are configured 34. When you use the Global Properties’ default settings on R76, which type of traffic will be

dropped if NO explicit rule allows the traffic? Ans. RIP traffic

35. R75 kernel resides directly below which layer of the OSI model? Note:

Application is the top and Physical is the bottom of the IP stack. Ans. Network 36. What physical machine must have access to the User Center public IP address when checking for

new packages with SmartUpdate? Ans. SmartUpdate GUI PC 37. you can change the system to 32-bit or 64-bit using the command

Ans. Set edition 38. the internal certificate authority (ica) cannot be used for

Ans. NAT rules 39. what are the dynamic routing protocol checkpoint r77 gaia os supports

Ans. OSPF 40. The SIC certificate is stored in the directory

Ans. $CPDIR/conf

Extra..

41. which command should run to check the status of corexl on your security gateway

Ans. fw6 ctl multik stat. 42. the certificate authority manager process and this process does not run on a multiple domain

log server or multiple domain server Ans. Fwm\_mds 43. Which specific R70 GUI would you use to view the length of time a TCP connection was open?

Ans. SmartView Monitor 44. Which of these attributes would be critical for a site-to-site VPN?

Ans. Strong data encryption 45. The script for the automatic start of Multi-Domain Server processes upon boot can be found in

Ans. /etc/init.d. The name of the file is firewall1. A link to this file appears in /etc/rc3.d directory under the name S95firewall1. 46. How is CheckPoint stateful-inspection firewalls provide a security measure against port

scanning? Ans. By closing all ports until the specific port is requested

Part 3

47. If you are experiencing LDAP issues , which of the following should you check

Ans. Connectivity between the NGX Gateway and LDAP server 48. Which of the following does the security Gateway R70 use of guaranteeing the integrity and

authenticity of message Ans. Digital signatures 49. The SIC certificate is stored in the directory

Ans. $CPDIR/conf 50. The most recommended and manageable method for authentication among Gateways and

Remote clients is Ans. Digital certificates 51. Web server child deamon

Ans. Httpd2 52. Which command displays the installed Security Gateway Version?

Ans. fw ver 53. What are the components are available in the security rule

Ans. Source IP 54. Which of the following is TRUE concerning unnumbered VPN Tunnel Interfaces(VTIs)?

Ans. VITS are only supported on Secured Platform. 55. Which of these attributes would be critical for a site –to-site VPN?

Ans. Strong data encryption 56. When Checkpoint product is used to create and save changes to a Log consolidation policy?

Ans. SmartDashboard Log Consolidator 57. Logging information on the Anti-Virus scan is sent to the Security management server and can

be viewed using which of the following GUI? Ans. SmartView Tracker 58. Before Security Gateways can exchange encryption keys and build VPN tunnels , they first need

to authenticate to each other. What are the types of credentials? Ans. Certificates 59. What is the purpose of stealth rule in the Rule base of VPN/Firewall?

Ans.It is the first rule in the Rule Base that prevents traffic from directly accessing the firewall itself. 60. The customer has a small Check Point installation which includes one Windows XP workstation

as a smartConnector Server,and the third server running SecurePlatform as Security Gateway.This is an example of a(n): Ans. 61. SmartView Tracker logs the following Security Administrator activities , EXCEPT:

Ans. Tracking SLA compliance. 62. Wait mode is a Client Authentication feature for Manual Sign On. What port number the user

initiates a client authenticated. Ans. 259 63. How do you enforces a strict change control policy . Which of the following would be MOST

effective for quickly dropping Ans. Block Intruder feature of SmartView Tracker 64. Multi Domain Server Installation creates subdirectories under

Ans. var/opt 65. When translation occurs using automatic Hide NAT. What also happens?

Ans.The source port is modified. 66. Where can an administrator configure the notification action in the event of a policy install time

change? Ans. Smartview monitor: Global Thresholds 67. What are the server platforms checkpoint multi domain server support

Ans. Checkpoint secure platform 68. How many timesis the firewall kernel invoked for a packet to be passed through a VPN

connection? Ans. One time

69. What ... is used to backs up binaries and data from your multi domain server to the working

directory Ans. Mds\_backup 70. What are the software version supported for the checkpoint 2200 appliance

Ans. R77 71. What is the command to check the number of connection passing throw the firewall

Ans. FW connection