KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **156-215.71**

Title : Check Point Certified Security Administrator R71 Version: 5.0

Version : DEMO

1.If you check the box Use Aggressive Mode in the IKE Properties dialog box, the standard:
A.three-packet IKE Phase 2 exchange Is replaced by a six-packet exchange
B.three-packet IKE Phase 2 exchange is replaced by a two-packet exchange
C.six-packet IKE Phase 1 exchange is replaced by a three-packet exchange
D.three-packet IKE Phase 1 exchange is replaced by a six-packet exchange
Answer: C

2.Of the following, what parameters will not be preserved when using Database Revision Control?
1) Simplified mode Rule Bases
2) Traditional mode Rule Bases
3) Secure Platform WebUI Users
4) SIC certificates
5) SmartView Tracker audit logs
6) SmartView Tracker traffic logs
7) Implied Rules
8) IPS Profiles
9) Blocked connections
10) Manual NAT rules
11) VPN communities
12) Gateway route table
13) 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

3.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: C

4.You are running a R71 Security Gateway on SecurePlatform, in case of a hardware failure.You have a server with the exact same hardware and firewall version Installed.What backup method could be used to quickly put the secondary firewall into production?
A.Upgrade_export
B.Manual backup
C.Snapshot
D.Backup
Answer: C

5.Your company is still using traditional mode VPN configuration on all Gateways and policies.Your manager now requires you to migrate to a simplified VPN policy to benefit from the new features.
This needs to be done with no downtime due to critical applications which must run constantly.How would you start such a migration?
A.This cannot be done without downtime as a VPN between a traditional mode Gateway and a simplified mode Gateway does not work.
B.You first need to completely rewrite all policies in simplified mode and then push this new policy to all Gateways at the same time.
C.This can not be done as it requires a SIC- reset on the Gateways first forcing an outage.
D.Convert the required Gateway policies using the simplified VPN wizard, check their logic and then migrate Gateway per Gateway.
Answer: D

6.What physical machine must have access to the User Center public IP address when checking for new packages with smartUpdate?
A.SmartUpdate GUI PC
B.SmartUpdate Repository SQL database Server
C.A Security Gateway retrieving the new upgrade package
D.SmartUpdate installed Security Management Server PC
Answer: A

7.In SmartView Tracker, which rule shows when a packet is dropped due to anti-spoofing?
A.Blank field under Rule Number
B.Rule 0
C.Cleanup Rule
D.Rule 1
Answer: B

8.The URL Filtering Policy can be configured to monitor URLs in order to:
A.Log sites from blocked categories.
B.Redirect users to a new URL.
C.Block sites only once.
D.Alert the Administrator to block a suspicious site.
Answer: A

9.The Customer has a small Check Point installation which includes one Windows XP workstation as SmartConsole, one Solaris server working as security Management Server, and a third server running SecurePlatform as Security Gateway.This is an Example of a (n):
A.Stand-Alone Installation.
B.Unsupported configuration
C.Distributed Installation
D.Hybrid Installation.
Answer: C

10.You want to implement Static Destination NAT in order to provide external, Internet users access to an internal Webserver that has a reserved (RFC 1918) IP address You have an unused valid IP address on the network between your Security Gateway and ISP router.You control the router that sits between the external interface of the firewall and the Internet.What is an alternative configuration if proxy ARP cannot be used on your Security Gateway?
A.Place a static host route on the firewall for the valid IP address to the internal Web server.
B.Place a static ARP entry on the ISP router for the valid IP address to the firewall's external address.
C.Publish a proxy ARP entry on the ISP router instead of the firewall for the valid IP address.
D.Publish a proxy ARP entry on the internal Web server instead of the firewall for the valid IP address.
Answer: B

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

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.
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

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

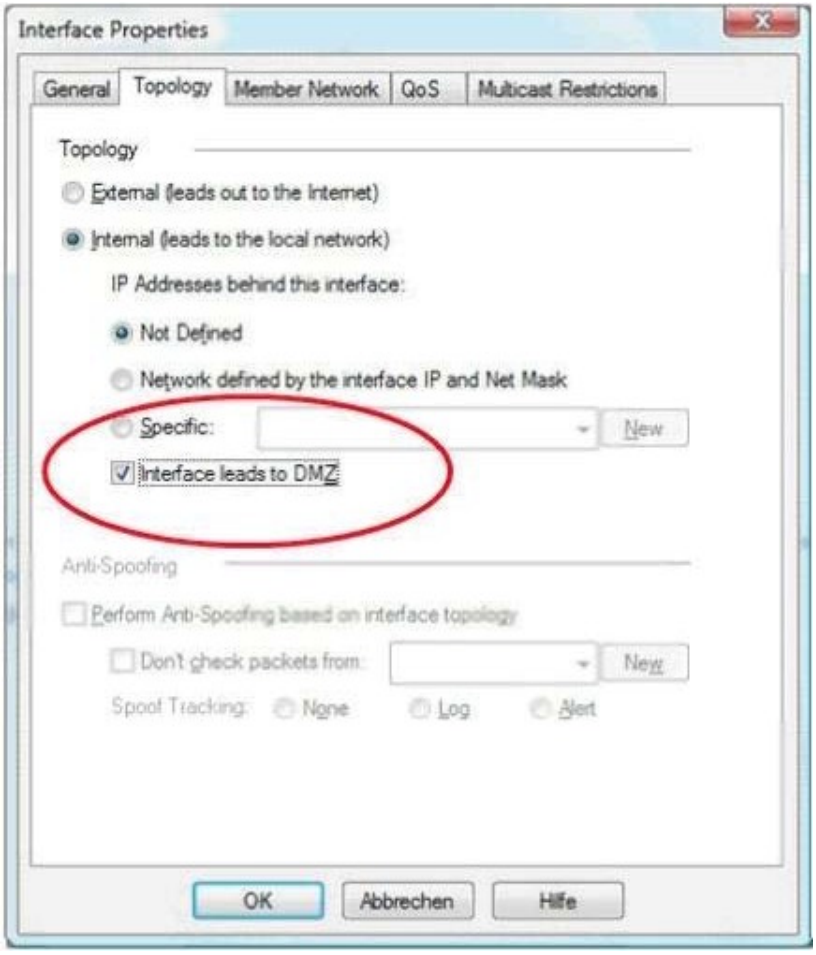
14.Phase 1 uses_____.
A.Conditional
B.Sequential
C.Asymmetric
D.Symmetric

Answer: C

15.An advantage of using central instead of local licensing is:
A.A license can be taken from one Security Management server and given to another Security Management Server.
B.Only one IP address is used for all licenses.
C.Licenses are automatically attached to their respective Security Gateways.
D.The license must be renewed when changing the IP address of security Gateway.Each module's license has a unique IP address.
Answer: B

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

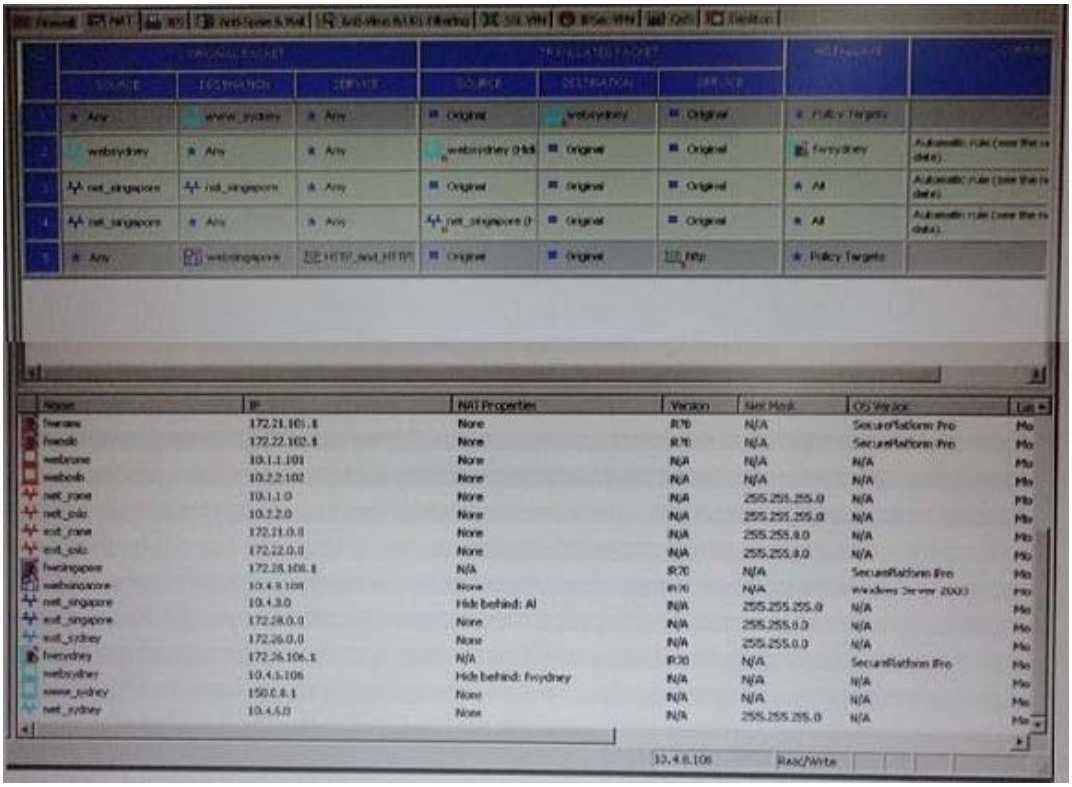
17.When configuring the network interfaces of a checkpoint Gateway, the direction can be defined as Internal or external.
What is meaning of interface leading to DMZ?



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

18.For which service is it NOT possible to configure user authentication?
A.HTTPS
B.FTP
C.SSH
D.Telnet
Answer: C

19.You have created a rule Base Firewall, websydney.Now you are going to create a new policy package with security and address transaction rules for a secured gateway.What is true about the new package's NAT rules?



A.Rules 1 and 5 will be appear in the new package
B.Rules 1, 3, 4and 5 will appear in the new package
C.Rules 2, 3 and 4 will appear in the new package
D.NAT rules will be empty in the new package
Answer: C

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

21.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

22.Which answers are TRUE? Automatic Static NAT CANNOT be used when:
i) NAT decision is based on the destination port
ii) Source and Destination IP both have to be translated
iii) The NAT rule should only be installed on a dedicated Gateway only
iv) NAT should be performed on the server side
A.(i), (ii), and (iii)
B.(i), and (ii)
C.ii) and (iv)
D.only (i)
Answer: D

23.Security Gateway R71 supports User Authentication for which of the following services? Select the response below that contains the most complete list of supported services.
A.FTP, HTTP, TELNET
B.FTP, TELNET
C.SMTP, FTP, HTTP, TELNET
D.SMTP, FTP, TELNET
Answer: A

24.Which of these security policy changes optimize Security Gateway performance?
A.Use Automatic NAT rules instead of Manual NAT rules whenever possible
B.Putting the least-used rule at the top of the Rule Base
C.Using groups within groups in the manual NAT Rule Base
D.Using domain objects in rules when possible
Answer: A

25.A Web server behind the Security Gateway is set to Automatic Static NAT.Client side NAT is not checked in the Global Properties.A client on the Internet initiates a session to the Web Server.Assuming there is a rule allowing this traffic, what other configuration must be done to allow the traffic to reach the Web server?
A.Automatic ARP must be unchecked in the Global Properties.

B.A static route must be added on the Security Gateway to the internal host.
C.Nothing else must be configured.
D.A static route for the NAT IP must be added to the Gateway's upstream router.
Answer: B

26.Latency has lost SIC communication with her Security Gateway and she needs to re establish SIC.What would be the correct order of steps needed to perform this task?
1) Create a new activation key on the Security Gateway, then exit cpconfig.
2) Click the Communication tab on the Security Gateway object, and then click Reset.
3) Run the cpconfig tool, and then select Secure Internal Communication to reset.
4) Input the new activation key in the Security Gateway object, and then click initialize
5) Run the cpconfig tool, then select source Internal Communication to reset.
A.5, 4, 1, 2
B.2, 3, 1, 4
C.2, 5, 1, 4
D.3, 1, 4, 2
Answer: B

27.Which type of resource could a Security Administrator use to control access to specific file shares on target machines?
A.URI
B.CIFS
C.Telnet
D.FTP
Answer: B

28.Which port must be allowed to pass through enforcement points in order to allow packet logging to operate correctly?
A.514
B.256
C.257
D.258
Answer: C

29.While in Smart View Tracker, Brady has noticed some very odd network traffic that he thinks could be an intrusion.He decides to block the traffic for 60 but cannot remember all the steps.What is the correct order of steps needed to perform this?
1) Select the Active Mode tab In Smart view Tracker
2) Select Tools > Block Intruder
3) Select the Log Viewing tab in SmartView Tracker
4) Set the Blocking Time out value to 60 minutes
5) Highlight the connection he wishes to block
A.3, 2, 5, 4
B.3, 5, 2, 4

C.1, 5, 2, 4
D.1, 2, 5, 4
Answer: C

30.A rule _____ is designed to log and drop all other communication that does not match another rule?
A.Stealth
B.Cleanup
C.Reject
D.Anti-Spoofing
Answer: B