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 : **156-215**

Title : Check Point Security Administration NGX

Version : DEMO

1 . What do you configure to launch an application when certain traffic goes through certain rules?
A . SNMP trap alert script
B . User-defined alert script
C . Custom scripts cannot be executed through alert scripts.
D . Pop-up alert script
Answer : B

2 . Users are not prompted for authentication when they access their Web servers, even though you have created an HTTP rule via User Authentication. Why?
A . Anna has forgotten to place the User Authentication Rule before the Stealth Rule.
B . Users must use SecuRemote Client, to use the User Authentication Rule.
C . Another rule that accepts HTTP without authentication exists in the Rule Base.
D . Anna checked the "cache password on desktop" option in Global Properties.
Answer : C

3 . You have blocked an IP address via the Block Intruder feature of SmartView Tracker. How can you see the addresses you have blocked?
A . Run fw sam M ij all on the gateway.
B . Run fwm blocked_view.
C . In SmartView Status click the Blocked Intruder tab.
D . In SmartView Tracker, click the Active tab, and the actively blocked connections display.
Answer : A

4 . You create implicit and explicit rules for the following network. The group object "internal-networks" includes networks 10.10.10.0 and 10.10.20.0. Assume "Accept ICMP requests" is enabled as before last in the Global Properties.
A . dropped by rule 2, the Cleanup Rule.
B . dropped by the last implicit rule.
C . dropped by rule 0.
D . accepted by rule 1.
Answer : D

5 . What is an alternative configuration if proxy ARP cannot be used on your Security Gateway?
A . Create a Suspicious Activity Rule in SmartView Monitor.
B . Publish a proxy ARP entry on the ISP router instead of the firewall for the valid IP address.
C . Publish a proxy ARP entry on the internal web server instead of the firewall for the valid IP address.
D . Place a static route on the firewall from the valid IP address to the internal web server.
Answer : A

6 . What do you use to view a VPN-1 NGX Security Gateway's status, including CPU use, amount of virtual memory, percent of free hard-disk space, and version?
A . SmartUpdate
B . SmartView Monitor
C . SmartView Tracker

D . SmartView Status
Answer : B

7 Which type of VPN-1 NGX Security Server does not provide User Authentication?
A . HTTP Security Server
B . SMTP Security Server
C . HTTPS Security Server
D . NNTP Security Server
Answer : B

8 You are a security consultant for a hospital. You are asked to create some type of authentication rule on the VPN-1 NGX Security Gateway, to allow doctors to update patients' records via HTTP from various workstations. Which authentication method should you use?
A . User Authentication
B . SecureID Authentication
C . Client Authentication
D . LDAP Authentication
Answer : A

9 . All VPN-1 NGX Security Servers can perform User authentication with the exception of one. Which of the Security Servers cannot perform User authentication?
A . FTP
B . HTTP
C . SMTP
D . RLOGIN
Answer : C

10 . You are working in a large hospital, together with three other Security Administrators. How do you use SmartConsole to check changes to rules or object properties other administrators made?:
A . Eventia Monitor
B . Eventia Tracker
C . SmartView Tracker
D . SmartView Monitor
Answer : C

11 . Which VPN-1 NGX feature or command allows Security Administrators to revert to earlier versions of the Security Policy without changing object configurations?
A . fwm dbexport/fwm dbimport
B . Database Revision Control
C . Policy Package management
D . upgrade_export/upgrade_import
Answer : C

12 . There is a Web server behind your perimeter Security Gateway. You need to protect the server from

network attackers, who create scripts that force your Web server to send user credentials or identities to other Web servers. Which box do you check in the SmartDashboard Web Intelligence tab?
A . Command Injection protection
B . SQL Injection protection
C . HTTP protocol inspection protection
D . Cross Site Scripting protection
Answer : D

13 . When you find a suspicious connection from a problematic host, you want to block everything from that whole network, not just the host. You want to block this for an hour, but you do not want to add any rules to the Rule Base. How do you achieve this?
A . Create a "FW SAM" rule in SmartView Monitor.
B . Create a "FW SAM" rule in SmartView Tracker > Tools menu.
C . Select "block intruder" from the Tools menu in the SmartView Tracker.
D . Create a Suspicious Activity Rule in SmartView Monitor.
Answer : D

14 . After implementing Static Address Translation to allow Internet traffic to an internal Web Server on your DMZ, you notice that any NATed connections to that machine are being dropped in the due anti-spoofing protections.
Which of the following is the most likely cause
A . The Global Properties setting "Translate destination on client side" is checked. The topology on the DMZ interface is set to "Internal Network defined by IP and Mask". Uncheck the Global Properties setting "Translate destination on client side".
B . The Global Properties setting "Translate destination on client side" is unchecked. The topology on the DMZ interface is set to "Internal Network defined by IP and Mask". Check the Global Properties setting "Translate destination on client side".
C . The Global Properties setting "Translate destination on client side" is unchecked. The topology on the external interface is set to "Others +". Change topology to "External"
D . The Global Properties setting "Translate destination on client side" is checked. The topology on the external interface is set to "External". Change topology to "Others +".
Answer : B

15 . Assuming the appropriate SmartView Monitor settings have been selected in SmartDashboard, how do you use SmartView Monitor to compile data for packet size distribution for your company's Internet activity during production hours? By:
A . selecting the "Traffic" view in SmartView Monitor to generate graphs showing the packet sizes.
B . selecting the "Tunnels" view, and generating a report on the statistics
C . configuring a Suspicious Activity Rule which triggers an alert when large packets pass through the Gateway
D . viewing total packets passed through the Security Gateway
Answer : A
16 . VPN-1 NGX uses _____ to retrieve the Interface Name, IP Address, and Network Mask when an administrator clicks the GET button in the Interfaces tab of an Externally Managed VPN Gateway

object.
A . ioctl
B . Control Connection
C . SNMP
D . URI
Answer : C

17 . Your online bookstore has customers connecting to a variety of Web servers to place or change orders, and check order status.
You ran penetration tests through the Security Gateway, to determine if the Web servers were protected from a recent series of cross-site scripting attacks.
The penetration testing indicated the Web servers were still vulnerable.
You have enabled every protection in the Web Intelligence branch, configured the protections to apply to all HTTP traffic, and installed the Security Policy.
What else might you do to reduce the vulnerability?
A . Check the "Products > Web Server" box on the host node objects representing your Web servers.
B . The penetration software you are using is malfunctioning and is reporting a false-positive.
C . Configure a URI to strip Script tags from HTTP requests, and use it in a rule allowing HTTP traffic to the web servers.
D . Configure the Security Gateway protecting the Web servers as a Web server.
Answer : C

18 . In SmartDashboard, you configure 45 MB as the required free hard-disk space to accommodate logs.
What can you do to keep old log files, when free space falls below 45 MB?
A . Do nothing. The SmartCenter Server archives old logs to another directory.
B . Use FTP to send the logs to another server.
C . Use the fwm logexport command to export the old log files to other location.
D . Define a secondary SmartCenter Server as a log server, to transfer the old logs.
Answer : B

19 . Larry is the Security Administrator for the CodeMore software-development company. To isolate the corporate network from the developers' network, Larry installs an internal Security Gateway. Larry wants to optimize the performance of this Gateway.
Which of the following actions is most likely to improve the Gateway's performance?
A . Remove unused Security Policies from Policy Packages.
B . Use domain objects in rules, where possible.
C . Clear all Global Properties check boxes, and use explicit rules.
D . Put the least-used rules at the top of the Rule Base.
Answer : A

20 . MegaCorp's security infrastructure separates Security Gateways geographically. You must request a central license for one remote Security Gateway. You must request a central license:
A . using the remote Gateway's IP address. Attach the license to the remote Gateway via SmartUpdate.
B . using your SmartCenter Server's IP address. Attach the license to the remote Gateway via

SmartUpdate.
C . using the remote Gateway's IP address. Apply the license locally with the cplic put command.
D . for the Gateways' IP addresses. Apply the licenses on the SmartCenter Server with the cprlic put command.
Answer : B