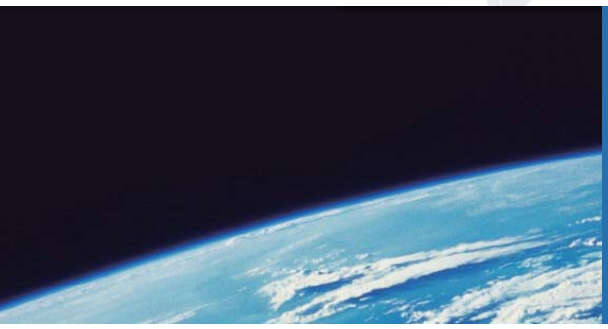
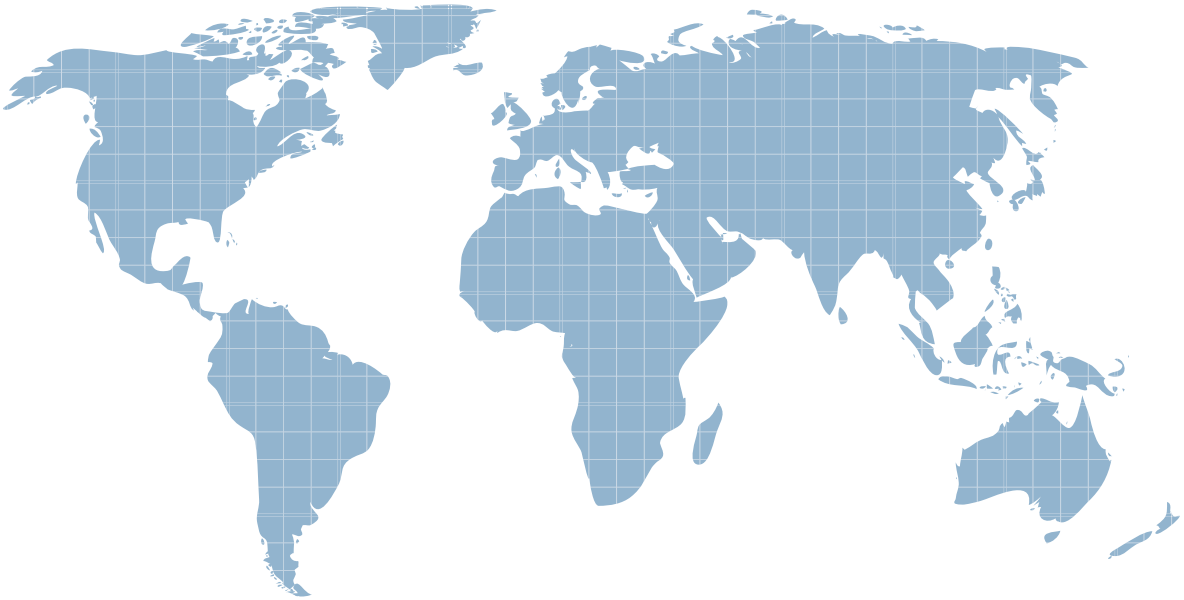


ITTEST

QUESTION & ANSWER

Guías de estudio precisos, Alta tasa de paso!



Ittest ofrece información actualizada de forma gratuita en un año!

http://www.ittest.es/

Exam : **156-915.65**

Title : Accelerated CCSE NGX R65

Version : DEMO

1.When upgrading to NGX R65, which Check Point products do not require a license upgrade to be current?
A.None, all versions require a license upgrade
B.VPN-1 NGX (R64) and later
C.VPN-1 NGX (R60) and later
D.VPN-1 NG with Application Intelligence (R54) and later
Answer:C
2.A security audit has determined that your unpatched web application server is revealing the fact that it accesses a SQL server. You believe that you have enabled the proper SmartDefense setting but would like to verify this fact using SmartView Tracker. Which of the following entries confirms the proper blocking of this leaked information to an attacker?
A."Fingerprint Scrambling: Changed [SQL] to [Perl]"
B."HTTP response spoofing: remove signature [SQL Server]"
C."Concealed HTTP response [SQL Server]. (Error Code WSE0160003)"
D."ASCII Only Response Header detected: SQL"
Answer:C
3.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 checked every box in the Web Intelligence tab, and installed the Security Policy. What else might you do to reduce the vulnerability?
A.Configure the Security Gateway protecting the Web servers as a Web server.
B.Check the "Products > Web Server" box on the host node objects representing your Web servers.
C.Configure resource objects as Web servers, and use them in the rules allowing HTTP traffic to the Web servers.
D.The penetration software you are using is malfunctioning and is reporting a false-positive.
Answer:C
4.Where is it necessary to configure historical records in SmartView Monitor to generate Express reports in Eventia Reporter?
A.In SmartDashboard, the SmartView Monitor page in the VPN-1 Security Gateway object
B.In Eventia Reporter, under Express > Network Activity
C.In Eventia Reporter, under Standard > Custom
D.In SmartView Monitor, under Global Properties > Log and Masters
Answer:A
5.Where do you enable popup alerts for SmartDefense settings that have detected suspicious activity?
A.In SmartView Monitor, select Tools > Alerts
B.In SmartView Tracker, select Tools > Custom Commands
C.In SmartDashboard, edit the Gateway object, select SmartDefense > Alerts
D.In SmartDashboard, select Global Properties > Log and Alert > Alert Commands
Answer:A
6.When configuring VPN High Availability (HA) with MEP, which of the following is correct?
A.The decision on which MEP Security Gateway to use is made on the remote gateway's side (non-MEP side).

B.MEP Gateways must be managed by the same SmartCenter Server.
C.MEP VPN Gateways cannot be geographically separated machines.
D.If one Gateway fails, the synchronized connection fails over to another Gateway and the connection continues.
Answer:A
7.Which Check Point product is used to create and save changes to a Log Consolidation Policy?
A.Eventia Reporter Client
B.SmartDashboard Log Consolidator
C.SmartCenter Server
D.Eventia Reporter Server
Answer:B
8.Which of the following would NOT be a reason for beginning with a fresh installation of VPN-1 NGX R65, instead of upgrading a previous version to VPN-1 NGX R65?
A.You see a more logical way to organize your rules and objects.
B.You want to keep your Check Point configuration.
C.Your Security Policy includes rules and objects whose purpose you do not know.
D.Objects and rules' naming conventions have changed over time.
Answer:B
9.How do you block some seldom-used FTP commands, such as CWD, and FIND from passing through the Gateway?
A.Use FTP Security Server settings in SmartDefense.
B.Add the restricted commands to the aftpd.conf file in the SmartCenter Server.
C.Configure the restricted FTP commands in the Security Servers screen of the Global properties.
D.Enable FTP Bounce checking in SmartDefense.
Answer:A
10.Match each of the following commands to their correct function. Each command only has one function listed.

C1: `cp_admin_convert`	F1: export and import different revisions of the database
C2: `cpca_client`	F2: Export and import policy packages
C3: `cp_merge`	F3: transfer Log data to an external database.
C4: `cpwd_admin`	F4: execute operations on the ICA
	F5: invokes and monitors critical processes such as Check Point daemons on the local machine.
	F6: automatically export administrator definitions that were created in `cpconfig` to SmartDashboard.

A.C1>F6; C2>F4; C3>F2; C4>F5
B.C1>F4; C2>F6; C3>F3; C4>F2
C.C1>F2; C2>F4; C3>F1; C4>F5

D.C1>F2; C2>F1; C3>F6; C4>F4

Answer:A

11.In ClusterXL, which of the following are defined by default as critical devices?

A.Security Policy status

B.fw.d

C.protect.exe

D.PROT_SRV.EXE

Answer:A

12.When a user selects to allow Hotspot, SecureClient modifies the Desktop Security Policy and/or Hub Mode routing to enable Hotspot registration. Which of the following is NOT true concerning this modification?

A.The modification is restricted by time.

B.The number of IP addresses accessed is not restricted.

C.IP addresses accessed during registration are recorded.

D.Ports accessed during registration are recorded.

Answer:B

13.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.Users must use the SecuRemote Client, to use the User Authentication Rule.

B.You have forgotten to place the User Authentication Rule before the Stealth Rule.

C.You checked the "cache password on desktop" option in Global Properties.

D.Another rule that accepts HTTP without authentication exists in the Rule Base.

Answer:B

14.When launching SmartDashboard, what information is required to log into VPN-1 NGX R65?

A.User Name, Password, SmartCenter Server IP

B.User Name, SmartCenter Server IP, certificate fingerprint file

C.Password, SmartCenter Server IP, LDAP Server

D.Password, SmartCenter Server IP

Answer:B

15.Which command line interface utility allows the administrator to verify the name and timestamp of the Security Policy currently installed on a firewall module?

A.fw ver

B.fw stat

C.fw ctl pstat

D.cpstat fwd

Answer:B

16.When configuring numbered VPN Tunnel Interfaces (VTIs) in a clustered environment, what issues need to be considered? (1) Each member must have a unique source IP address (2) Every interface on each member requires a unique IP address (3) All VTIs going to the same remote peer must have the same name. (4) Custer IP addresses are required.

A.2 & 3

B.1, 3, & 4

C.1, 2, 3 & 4

D.1, 2, and 4

Answer:C

17.You are reviewing the Security Administrator activity for a bank and comparing it to the change log. How do you view Security Administrator activity?

A.SmartView Tracker in Active Mode

B.SmartView Tracker in Audit Mode

C.SmartView Tracker cannot display Security Administrator activity; instead, view the system logs on the SmartCenter Server's Operating System.

D.SmartView Tracker in Log Mode

Answer:B

18.Match the remote-access VPN Connection mode features with their descriptions:

A. Office Mode	1. E-mail client tries to access an IMAP server behind the Security Gateway, SecureClient prompts the user to initiate a tunnel to that Gateway.
B. Visitor Mode	2. Resolves routing issues between the client and the Gateway
C. Hub Mode	3. Tunnels client-to-Gateway traffic via TCP on port 443
D. Auto Connect	4. All traffic routed through the Gateway

A.A 3, B 4, C 2, D 1

B.A 2, B 3, C 4, D 1

C.A 2, B 4, C 3, D 1

D.A 1, B 3, C 4, D 2

Answer:B

19.How do you recover communications between your SmartCenter Server and Security Gateway if you "lock" yourself out via a rule or policy mis-configuration?

A.cpstop

B.fw unload policy

C.fw delete all.all

D.fw unloadlocal

Answer:D

20.Which operating system is not supported by SecureClient?

A.MacOS X

B.Windows XP SP2

C.Windows 2003 Professional

D.IPSO 3.9

Answer:D