156-210

CheckPoint

VPN-1/FireWall-1 Management I NG

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 156-210 exam in first attempt and also get high scores to acquire CheckPoint certification.

If you use OfficialCerts 156-210 Certification questions and answers, you will experience actual 156-210 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our CheckPoint exam prep covers over 95% of the questions and answers that may be appeared in your 156-210 exam. Every point from pass4sure 156-210 PDF, 156-210 review will help you take CheckPoint 156-210 exam much easier and become CheckPoint certified.

Here's what you can expect from the OfficialCerts CheckPoint 156-210 course:

** Up-to-Date CheckPoint 156-210 questions as experienced in the real exam.*
** 100% correct CheckPoint 156-210 answers you simply can't find in other 156-210 courses.*
** All of our tests are easy to download. Your file will be saved as a 156-210 PDF.*
** CheckPoint 156-210 brain dump free content featuring the real 156-210 test questions.*

CheckPoint 156-210 certification exam is of core importance both in your Professional life and CheckPoint certification path. With CheckPoint certification you can get a good job easily in the market and get on your path for success. Professionals who passed CheckPoint 156-210 exam training are an absolute favorite in the industry. You will pass CheckPoint 156-210 certification test and career opportunities will be open for you.

http://janetdailey.com/?certs=exams.asp?examcode=156-210

156-210

QUESTION 1
Once you have installed Secure Internal Communcations (SIC) for a host-node object and issued a certificate for it. Which of the following can you perform? Choose two.

A. Rename the object
B. Rename the certificate
C. Edit the object properties
D. Rest SIC
E. Edit the object type

Answer: A, C

Explanation:
Object can be renamed and the properties can be edited even after establishing the SIC and issue the certificate
Incorrect Answers:
B. Once SIC has been established and a certificate has been issued, certificate can not be renamed
D. If SIC is reset, the trust has to be re-established, hence this is wrong
E. Type of the object created can not be modified once the certificate has been issued.

QUESTION 2
You are a Security Administrator preparing to implement Hide NAT. You must justify your decision. Which of the following statements justifies implementing a Hide NAT solution? Choose two.

A. You have more internal hosts than public IP addresses
B. Your organization requires internal hosts, with RFC 1918-compliant addresses to be assessable from the Internet.
C. Internally, your organization uses an RFC 1918-compliant addressing scheme.
D. Your organization does not allow internal hosts to access Internet resources
E. Internally, you have more public IP addresses than hosts.

Answer: A, C

QUESTION 3
Which critical files and directories need to be backed up? Choose three

A. $FWDIR/conf directory
B. rulebase_5_0.fws
C. objects_5_0.c
D. $CPDIR/temp directory
E. $FWDIR/state directory

Answer: A, B, C

QUESTION 4
Which of the following statements about the General HTTP Worm Catcher is FALSE?

A. The General HTTP Worm Catcher can detect only worms that are part of a URI.
B. Security Administrators can configure the type of notification that will take place, if a worm is detected.
C. SmartDefense allows you to configure worm signatures, using regular expressions.
D. The General HTTP Worm Catcher's detection takes place in the kernel, and does not require a Security Server.
E. Worm patterns cannot be imported from a file at this time.

Answer: A

QUESTION 5
You are a Security Administrator attempting to license a distributed VPN-1/Firewall-1 configuration with three Enforcement Modules and one SmartCenter Server. Which of the following must be considered when licensing the deployment? Choose two.

A. Local licenses are IP specific.
B. A license can be installed and removed on a VPN-1/Firewall-1 version 4.1, using SmartUpdate.
C. You must contact Check Point via E-mail or telephone to create a license for an Enforcement Module.
D. Licenses cannot be installed through SmartUpdate.
E. Licenses are obtained through the Check Point User Center

Answer: A, E

QUESTION 6
Which of the following are tasks performed by a VPN-1/FireWall-1 SmartCenter Server? Choose three.

A. Examines all communications according to the Enterprise Security Policy.
B. Stores VPN-1/FirWall-1 logs.
C. Manages the User Database.
D. Replicates state tables for high availability.
E. Compiles the Rule Base into an enforceable Security Policy.

Answer: B, C, E

QUESTION 7
You are a Security Administrator preparing to implement an address translation solution for Certkiller .com.
The solution you choose must meet the following requirements:
1. RFC 1918-compliant internal addresses must be translated to public, external addresses when packets exit the Enforcement Module.
2. Public, external addresses must be translated to internal, RFC 1918-compliant addresses when packets enter the Enforcement Module.
Which address translation solution BEST meets your requirements?

A. Hide NAT
B. The requirements cannot be met with any address translation solution.
C. Dynamic NAT
D. IP Pool Nat
E. Static NAT

Answer: E

QUESTION 8
Which of the following suggestions regarding Security Policies will NOT improve performance?

A. If most incoming connections are HTTP, but the rule that accepts HTTP at the bottom of the Rule Base, before the Cleanup Rule
B. Use a network object, instead of multiple host-node objects.
C. Do not log unnecessary connections.
D. Keep the Rule Base simple.
E. Use IP address-range objects in rules, instead of a set of host-node objects.

Answer: A

QUESTION 9
You are a Security Administrator attempting to license a distributed VPN-1/Firwall-1 configuration with three Enforcement Modules and one SmartCenter Server. Which license type is the BEST for your deployemenet?

A. Discretionary
B. Remote
C. Central
D. Local
E. Mandatory

Answer: C

QUESTION 10
Network attacks attempt to exploit vulnerabilities in network applications, rather than targeting firewalls directly.
What does this require of today's firewalls?

A. Firewalls should provide network-level protection, by inspecting packets all layers of the OSI model.
B. Firewall should not inspect traffic below the Application Layer of the OSI model, because such inspection is no longer relevant.
C. Firewalls should understand application behavior, to protect against application attacks and hazards.
D. Firewalls should provide separate proxy processes for each application accessed through the firewall.
E. Firewalls should be installed on all Web servers, behind organizations' intranet.

Answer: C

QUESTION 11
What function does the Audit mode of SmartView Tracker perform?

A. It tracks detailed information about packets traversing the Enforcement Modules.
B. It maintains a detailed log of problems with VPN-1/FireWall-1 services on the SmartCenter Server.
C. It is used to maintain a record of the status of each Enforcement Module and SmartCenter server.
D. It maintains a detailed record of status of each Enforcement Module and SmartCenter Server.
E. It tracks changes and Security Policy installations, per Security Administrator, performed in SmartDashboard.

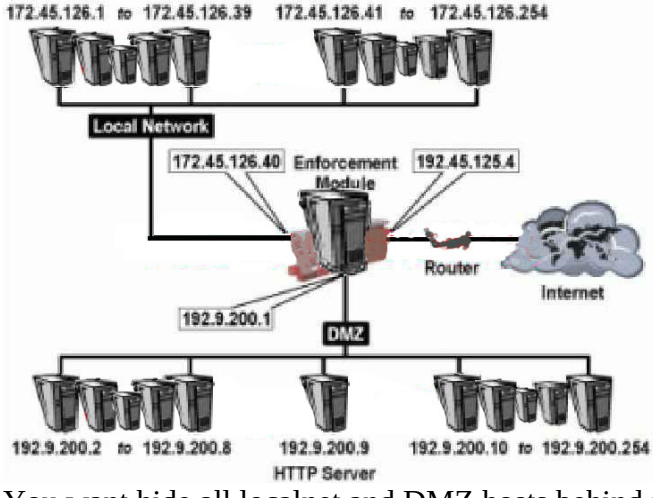
Answer: E

QUESTION 12
In the SmartView Tracker, what is the difference between the FireWall-1 and VPN-1 queries? Choose three.

A. A VPN-1 query only displays encrypted and decrypted traffic.
B. A FireWall-1 query displays all traffic matched by rules, which have logging activated.
C. A FireWall-1 query displays all traffic matched by all rules.
D. A FireWall-1 query also displays encryption and decryption information.
E. Implied rules, when logged, are viewed using the VPN-1 query.

Answer: A, B, D

QUESTION 13
Network topology exhibit



You want hide all localnet and DMZ hosts behind the Enforcemenet Module, except for the HTTP Server (192.9.200.9). The HTTP Server will be providing public services, and must be accessible from the Internet.
Select the two BEST Network Address Translation (NAT) solutions for this scenario,

A. To hide Local Network addresses, set the address translation for 192.9.0.0

B. To hide Local Network addresses, set the address translation for 192.9.200.0
C. Use automatic NAT rule creation to hide both DMZ and Local Network.
D. To hide Local Network addresses, set the address translation for privatenet.
E. Use automatic NAT rule creation, to statically translate the HTTP Server address.

Answer: C, E

QUESTION 14
The SmartDefense Storm Center Module agent receives the Dshield.org Block List, and:

A. Populates CPDShield with blocked address ranges, every three hours.
B. Generates logs from rules tracking internal traffic.
C. Submits the number of authentication failures, and drops, rejects, and accepts.
D. Generates regular and compact log digest.
E. Populates the firewall daemon with log trails.

Answer: A

QUESTION 15
What are the advantages of central licensing? Choose three.

A. Only the IP address of a SmartCenter Server is needed for all licences.
B. A central licence can be removed from one Enforcement Module, and installe don another Enforcement Module.
C. Only the IP address of an Enforcement Module is needed for all licences.
D. A central license remains valid, when you change the IP address of an Enforcemente Module.
E. A central license can be converted into a local license.

Answer: A, B, D

QUESTION 16
A security Administrator wants to review the number of packets accepted by each of the Enforcement modules. Which of the following viewers is the BEST source for viewing this information?

A. SmartDashboard
B. SmartUpdate
C. SmartMap
D. SmartView Status
E. SmartView Tracker

Answer: D

QUESTION 17
Hidden (or masked) rules are used to:

A. Hide rules from administrators with lower privileges.

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google