

Examcollection

<http://www.ipass4sure.com/examcollection.htm>



<http://www.ipass4sure.com>

156-210

CheckPoint

VPN-1/FireWall-1 Management I NG

<http://www.ipass4sure.com/exams.asp?examcode=156-210>

The 156-210 practice exam is written and formatted by Certified Senior IT Professionals working in today's prospering companies and data centers all over the world! The 156-210 Practice Test covers all the exam topics and objectives and will prepare you for success quickly and efficiently. The 156-210 exam is very challenging, but with our 156-210 questions and answers practice exam, you can feel confident in obtaining your success on the 156-210 exam on your FIRST TRY!

CheckPoint 156-210 Exam Features

- Detailed questions and answers for 156-210 exam
- Try a demo before buying any CheckPoint exam
- 156-210 questions and answers, updated regularly
- Verified 156-210 answers by Experts and bear almost 100% accuracy
- 156-210 tested and verified before publishing
- 156-210 examcollection vce questions with exhibits
- 156-210 same questions as real exam with multiple choice options

Acquiring CheckPoint certifications are becoming a huge task in the field of I.T. More over these exams like 156-210 exam are now continuously updating and accepting this challenge is itself a task. This 156-210 test is an important part of CheckPoint certifications. We have the resources to prepare you for this. The 156-210 exam is essential and core part of CheckPoint certifications and once you clear the exam you will be able to solve the real life problems yourself. Want to take advantage of the Real 156-210 Test and save time and money while developing your skills to pass your CheckPoint 156-210 Exam? Let us help you climb that ladder of success and pass your 156-210 now!

DEMO EXAM

For Full Version visit

<http://www.ipass4sure.com/allexams.asp>

QUESTION 1

Once you have installed Secure Internal Communications (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 deployment?

- 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

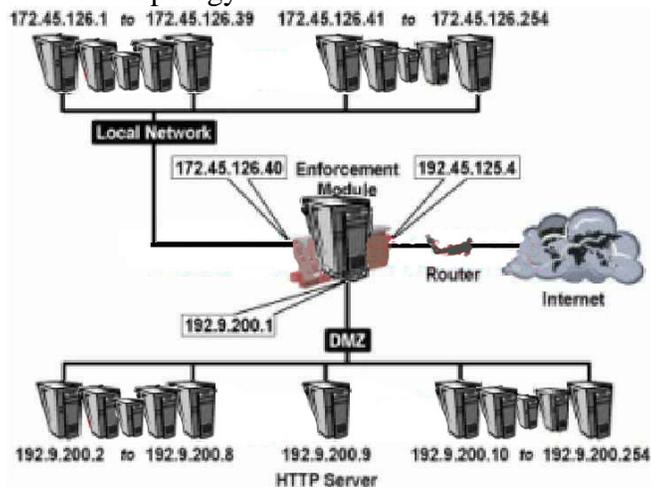
In the SmartView Tracker, what is the difference between the FireWall-1 and VPN-1 queries? Choose three.

- 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 Enforcement 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

156-210

- 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 installed on 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 Enforcement 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.



Pass4sure Certification Exam Features;

- Pass4sure offers over **2500** Certification exams for professionals.
- More than **98,800** Satisfied Customers Worldwide.
- Average **99.8%** Success Rate.
- Over **120** Global Certification Vendors Covered.
- Services of **Professional & Certified Experts** available via support.
- Free **90 days** updates to match real exam scenarios.
- **Instant Download Access!** No Setup required.
- Price as low as **\$19**, which is 80% more **cost effective** than others.
- **Verified answers** researched by industry experts.
- Study Material **updated** on regular basis.
- Questions / Answers are downloadable in **PDF** format.
- Mobile Device Supported (**Android, iPhone, iPod, iPad**)
- **No authorization** code required to open exam.
- **Portable** anywhere.
- **Guaranteed Success.**
- **Fast**, helpful support **24x7**.



View list of All certification exams offered;
<http://www.ipass4sure.com/all exams.asp>

View list of All Study Guides (SG);
<http://www.ipass4sure.com/study-guides.asp>

View list of All Audio Exams (AE);
<http://www.ipass4sure.com/audio-exams.asp>

Download Any Certification Exam DEMO.
<http://www.ipass4sure.com/samples.asp>

To purchase Full version of exam click below;
<http://www.ipass4sure.com/all exams.asp>

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	

and many others.. See complete list [Here](#)

