156-310

CheckPoint

Check Point NG with Application Intelligence - Management II

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 156-310 exam in first attempt and also get high scores to acquire CheckPoint certification.

If you use OfficialCerts 156-310 Certification questions and answers, you will experience actual 156-310 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 156-310 exam. Every point from pass4sure 156-310 PDF, 156-310 review will help you take CheckPoint 156-310 exam much easier and become CheckPoint certified.

Here's what you can expect from the OfficialCerts CheckPoint 156-310 course:

** Up-to-Date CheckPoint 156-310 questions as experienced in the real exam.*
** 100% correct CheckPoint 156-310 answers you simply can't find in other 156-310 courses.*
** All of our tests are easy to download. Your file will be saved as a 156-310 PDF.*
** CheckPoint 156-310 brain dump free content featuring the real 156-310 test questions.*

CheckPoint 156-310 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 156-310 exam training are an absolute favorite in the industry. You will pass CheckPoint 156-310 certification test and career opportunities will be open for you.

http://news.ift.org/?newsid=exams.asp?examcode=156-310

156-310

QUESTION 1:

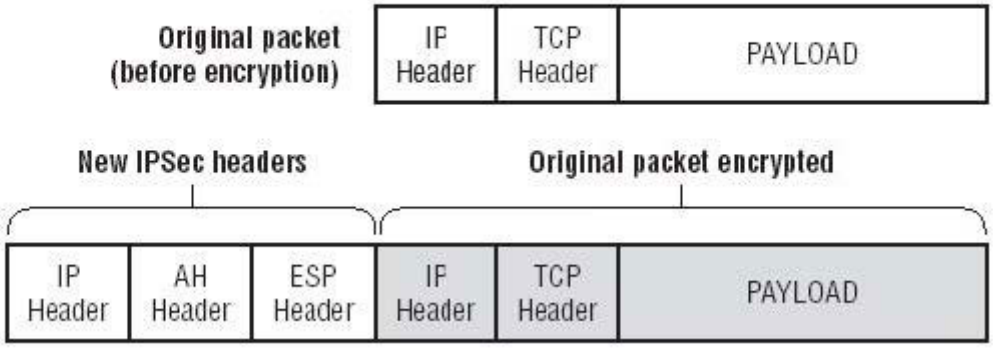
Which of the following statements about IKE Encryption are TRUE? (Choose three)

A. The final packet size is increased after it is encrypted.
B. TCP and IP headers are encrypted, along with the payload.
C. IKE uses in-place encryption.
D. IKE can use the FWZ1 encryption algorithm.
E. IKE uses tunneling encryption.

Answer: A, B, E

Explanation:
IKE Encryption Scheme
A long time ago (about four years in real time), Check Point supported many different encryption schemes: Manual IPSec, Simple Key Management for Internet Protocols (SKIP), FWZ (Check Point's own proprietary scheme), and Internet Key Exchange (IKE). As the industry began to settle on a standard and it became apparent that different vendors' VPN products needed to work together, the schemes were whittled down to only one: IKE.
IKE is a hybrid protocol that combines the Internet Security Association and Key Management Protocol (ISAKMP) and the Oakley Key Exchange Protocol. ISAKMP is responsible for the generation and maintenance of Security Associations, and Oakley is responsible for key exchanges. Both ISAKMP/Oakley and IKE are described in the IETF standard for encryption using the IP Security Protocol (IPSec). (The terms IKE and IPSec are frequently used interchangeably.)
You can find more on IPSec and its related protocols in RFCs 2401-2411 and 2451.
IPSec provides the access control, integrity of the packet, authentication, rejection of replayed packets, encryption, and non-repudiation (there's that PAIN acronym coming into play). IPSec does so by using the protocols Authentication Header (AH) and Encapsulating Security Payload (ESP). Each protocol-IPSec, AH, and ESP-is incorporated into its own header in the IPSec packet. IKE is also a tunneling protocol, which means it encrypts the entire original packet and adds new headers to the encrypted packet.

IPSec packet



Tunneling encrypts the entire original packet and adds new headers, which increases packet size and the likelihood of packet fragmentation. In-place encryption was Check Point's proprietary FWZ scheme supported in versions packet size did not increase. Although FWZ is no longer supported as of FP2, this information could still be used for a valid NG test question.
The new IP header uses the IPSec protocol and replaces the true source and destination of the packet (which are now encrypted) with the source and destination IP addresses of the firewalls involved in the VPN tunnel.
The AH header provides data integrity and authentication by using a message digest (instead of a digital signature, which is too slow for this process) and a Security Parameters Index (SPI). The SPI is like a pointer that tells your VPN partner which methods were selected for this VPN session. The SPI references the Security Association (SA), which was negotiated by the VPN participants. A good analogy to describe the SA is a large spreadsheet that contains all the possible combinations for key exchange, encryption, data integrity, and so forth that could be used for this connection. The SPI is the pointer that tells each partner which parts of the spreadsheet will be used for this specific tunnel.
The ESP header provides confidentiality as well as authentication. It gives a reference to the SPI as well as an Initialization Vector (IV), which is another data integrity check.
IKE supports a variety of different encryption algorithms, but VPN-1 supports only DES, Triple-DES, CAST, and AES.

Encryption Standards Support by IKE and VPN-1

Algorithm	Description
DES	Data Encryption Standard (standard in the U.S. for the last 20 years). A symmetric key encryption method that uses 56-bit keys.
Triple DES	A variation on DES that addresses the problem of short, easily breakable keys. Encrypts with three different DES keys in succession, which increases the effective key strength to 168 bits.

Encryption Standards Support by IKE and VPN-1 *(continued)*

Algorithm	Description
CAST	Named for its inventors, Carlisle Adams and Stafford Tavares. Similar to DES and supports variable key lengths from 40–128 bits.
AES	Advanced Encryption Standard. The new Federal Information Processing Standard (FIPS) standard. Also known as Rijndael (pronounced "rhine-doll") for its inventors, Vincent Rihmen and Joan Daemen.

For a more detailed explanation of encryption, IPSec, and cryptography, we recommend Applied Cryptography (John Wiley & Sons, 1995), RSA Security's Official Guide to Cryptography (McGraw-Hill, 2001) and IPSec Securing VPNs (McGraw-Hill Osborne Media, 2001).
Encryption is not an easy topic to grasp, especially in an abbreviated format within a study guide. But this background information is essential before we go into detail about how IKE negotiates keys and eventually encrypts data.
Let's forge ahead and tackle the IKE phases of key negotiation.

QUESTION 2:

When upgrading a configuration to NG with Application Intelligence: (Choose the FALSE answer)

A. Upgrade the SmartConsole.
B. Upgrade each module's version in SmartDashboard manually.

C. Upgrade the VPN-1/Firewall-1 Enforcement Modules.
D. Copy $FWDIR/state from one version of VPN-1/FireWall-1 to another version of VPN-1/FireWall-1.
E. Upgrade the SmartCenter server. The version is set during the upgrade.

Answer: D

Explanation:
Upgrading to VPN-1/FireWall-1 NG
Now that you've performed a successful installation of FireWall-1 NG, it's time to understand how to upgrade from a previous version of VPN-1/ FireWall-1. At the time of this writing, many companies are looking to upgrade from an older version of VPN-1/FireWall-1 (usually 4.1 SP3 or higher) to NG FP3. You can upgrade to NG FP1 from version 4.0 and higher. If you are running a version older than 4.0, you must upgrade to version 4.0 first, and then upgrade to NG.
With the many enhancements in NG, it's better to create a fresh install of NG and then migrate your existing configuration files over to the newly created NG firewall. The upgrade technique discussed here will upgrade version 4.1 Service Pack 6 configuration files to NG configuration files. It is recommended that the 4.1 files are upgraded to Service Pack 6 before convertingthem to NG.
In many instances, companies are viewing the NG upgrade as an opportunity to upgrade the current platform on which their firewalls are running.
For example, this is an chance to upgrade operating systems from Solaris 2.6 to 2.8, or to upgrade hardware from a Pentium II machine with limited hard drive space and memory to a Pentium IV with lots of hard drive space and much more memory.
In order to make the NG upgrade a smooth and convenient process, Check Point has developed an upgrade script that helps convert 4.1 configuration files to NG configuration files. This scripts automates the conversion by using the confmerge command on the objects.C, fwauth.NDB, and rulebases.fws files. (This script is not meant for people who are moving from a Windows machine to a Unix machine, or for people running Flood-Gate.) The script is in a zipped file called upgrade.4.3.tgz and can be downloaded from the support.checkpoint.com website. Here are the steps to use the upgrade script:
1. Create a new SmartCenterServer machine with the desired Feature Pack version of NG (FP1, FP2 or FP3), based on the installation guidelines previously discussed. This upgrade procedure will upgrade to FP3.
2. Download and unzip the upgrade.4.3.tgz file. This file opens into a directory named upgrade.
3. Place the 4.1 SP6 files on the SmartCenter Server under upgrade/4.1:
a. objects.C.
b. fwauth.NDB. On Windows machines, this file is only the pointer to the real database file-for example, fwauth.NDB522. In this case, take the real database file (fwauth.NDB522), rename it fwauth.NDB, and put it in the \upgrade\4.1 directory.

c. rulebases.fws.
4. Stop the FireWall-1 Services (cpstop), cd to the ,
and issue the following command
in Windows (upgrade from 4.1 to FP3):
upgrade.bat < upgrade_directory>\upgrade FP3 4.1
In Unix, enter this command (upgrade from 4.1 to FP3):
upgrade.csh < upgrade_directory>/upgrade FP3 4.1
5. Restart the FireWall Services (cpstart) and log in to the GUI.
After you have successfully run the script, in order to transfer the remaining configuration files (such as gui-clients, masters, and so on), copy the following files from the VPN-1/FireWall-1 4.1 $FWDIR/conf directory to the VPN-1/FireWall-1 NG $FWDIR/conf directory:
xlate.conf, aftpd.conf, smtp.conf, sync.conf, masters,
clients, fwmusers, gui-clients, slapd.conf, serverkeys,
product.conf
In addition to understanding which configuration files are important in upgrading to Check Point NG, it's important to understand which configuration files need to be saved for backup in case of a failure or loss of files. The next section talks about backup and restore options and identifies the critical configuration files needed for backup.

QUESTION 3:

When you upgrade VPN-1/FireWall-1, what components are carried over to the new version? (Choose two)

A. Licenses
B. VPN-1/FireWall-1 database
C. OPSEC database
D. Backward Compatibility
E. Rule Base

Answer: A, B

Explanation:
Upgrading to VPN-1/FireWall-1 NG
Now that you've performed a successful installation of FireWall-1 NG, it's time to understand how to upgrade from a previous version of VPN-1/ FireWall-1. At the time of this writing, many companies are looking to upgrade from an older version of VPN-1/FireWall-1 (usually 4.1 SP3 or higher) to NG FP3. You can upgrade to NG FP1 from version 4.0 and higher. If you are running a version older than 4.0, you must upgrade to version 4.0 first, and then upgrade to NG.
With the many enhancements in NG, it's better to create a fresh install of NG and then migrate your existing configuration files over to the newly created NG firewall. The upgrade technique discussed here will upgrade version 4.1

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