ISLEVER

156-310

CCSE NG

DEMO

https://www.islever.com/156-310.html

https://www.islever.com/checkpoint.html

QUESTION NO: 1

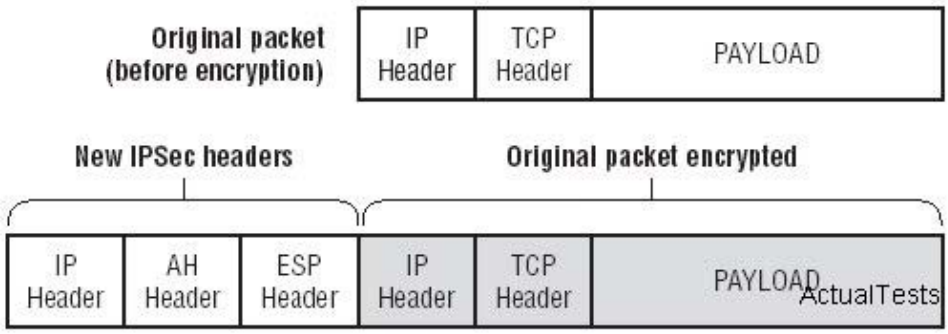
Which of the following statements about IKE Encryption are TRUE? (Choose three)

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 before FP2. It only encrypted the payload, and left the headers alone; therefore 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 NO: 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.