THE FIVE HIGH-LEVEL STEPS OF IPSEC

FOR THE CISSP EXAM

IPSec secures data in motion through confidentiality, integrity, authentication, and anti-replay.

STEP 1

Define the LAN IP addresses that will need to be secured within an IPSec VPN tunnel

This traffic will be known as "interesting traffic"

STEP 2

Internet Key Exchange (IKE) Phase 1 begins

The two peer devices authenticate each other by exchanging pre-shared keys

Encryption and hashing algorithms for IKE security association (SA) are negotiated between peers to provide confidentiality and integrity

Initiator and responder calculate a cookie value to protect against anti-replay attacks

Diffie-Hellman (DH) key exchange creates shared secret keys to secure IKE Phase 2

STEP 3

Internet Key Exchange (IKE) Phase 2 begins

Previous IKE SA protects the negotiation and establishment of IPSEC SA

Option to enable Perfect Forward Secrecy (PFS) for an additional DH key exchange

STEP 4

Data is sent over an encrypted tunnel

STEP 5

Tunnel is terminated either by manual deletion or an automatic lifetime setting

CORE CONCEPTS

IPSec has two options: Authentication Header (AH) and Encapsulating Security Payload (ESP)

IPSec, digital signatures, and PKI are some of the best topics to understand cryptography for the CISSP exam

STUDY NOTES AND THEORY | A CISSP STUDY GUIDE
WWW.STUDYNOTESANDTHEORY.COM