CiscoPress - IPSec VPN Design

The definitive design and deployment guide for secure virtual private networks

- Learn about IPSec protocols and Cisco IOS IPSec packet processing
- Understand the differences between IPSec tunnel mode and transport mode
- Evaluate the IPSec features that improve VPN scalability and fault tolerance, such as dead peer detection and control plane keepalives
- Overcome the challenges of working with NAT and PMTUD
- Explore IPSec remote-access features, including extended authentication, mode-configuration, and digital certificates
- Examine the pros and cons of various IPSec connection models such as native IPSec, GRE, and remote access
- Apply fault tolerance methods to IPSec VPN designs

- Employ mechanisms to alleviate the configuration complexity of a large- scale IPSec VPN, including Tunnel End-Point Discovery (TED) and Dynamic Multipoint VPNs (DMVPN)
- Add services to IPSec VPNs, including voice and multicast
- Understand how network-based VPNs operate and how to integrate IPSec VPNs with MPLS VPNs

Among the many functions that networking technologies permit is the ability for organizations to easily and securely communicate with branch offices, mobile users, telecommuters, and business partners. Such connectivity is now vital to maintaining a competitive level of business productivity. Although several technologies exist that can enable interconnectivity among business sites, Internet-based virtual private networks (VPNs) have evolved as the most effective means to link corporate network resources to remote employees, offices, and mobile workers. VPNs provide productivity enhancements, efficient and convenient remote access to network resources, site-to-site connectivity, a high level of security, and tremendous cost savings.

Download | **Size:** 8.85 MB