CiscoPress - Comparing, Designing, and Deploying VPNs

A practical guide for comparing, designing, and deploying IPsec, MPLS Layer 3, L2TPv3, L2TPv2, AToM, and SSL virtual private networks

- Explore the major VPN technologies and their applications, design, and configurations on the Cisco IOS® Router, Cisco® ASA 5500 Series, and the Cisco VPN 3000 Series Concentrator platforms
- Compare the various VPN protocols and technologies, learn their advantages and disadvantages, and understand their real-world applications and methods of integration
- Find out how to design and implement Secure Socket Layer (SSL) VPNs, including consideration of clientless operation, the Cisco SSL VPN Client, the Cisco Secure Desktop, file and web server access, e-mail proxies, and port forwarding
- Learn how to deploy scalable and secure IPsec and L2TP remote access VPN designs, including consideration of authentication, encryption, split-tunneling, high availability, load-balancing, and NAT transparency
- Master scalable IPsec site-to-site VPN design and implementation including configuration of security protocols and policies, multiprotocol/ multicast traffic transport, NAT/PAT traversal, quality of service (QoS), Dynamic Multipoint VPNs (DMVPNs), and public key infrastructure (PKI)

Virtual private networks (VPNs) enable organizations to connect offices or other sites over the Internet or a service provider network and allow mobile or home-based users to enjoy the same level of productivity as those who are in the same physical location as the central network. However, with so many flavors of VPNs available, companies and providers are often hard pressed to identify, design, and deploy the VPN solutions that are most appropriate for their particular network architecture and service needs.

Download | **Size:** 39.50 MB