15.11 VPN Access and Authentication

As you study this section, answer the following questions:

- What is a VPN's main purpose?
- What technology does SSL provide to a VPN?
- What technology does IPsec provide to a VPN?
- Which two modes does IPsec use? What are their differences?
- How does DTLS ensure that packets are delivered correctly?

Key terms for this section include the following:

Term	Definition
Virtual Private Network (VPN)	A type of network that uses encryption to allow IP traffic to travel securely over a TCP/IP network and is used primarily to support secure communications over an untrusted network.
Secure Sockets Layer (SSL)	The standard technology used for keeping an internet connection secure. It does this by encrypting the data sent between systems and using digital certificates to ensure that only the intended recipients can view and use the data sent.
Internet Protocol Security (IPsec)	Is an extension to the IP protocol and like SSL also secures sessions between computers by validating and encrypting the packets of data that are sent across a network.
Datagram Transport Layer Security (DTLS)	Provides security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The main difference between DTSL and Transport Layer Security (TLS) is that DTLS uses the User Datagram Protocol (UDP), and TLS uses the Transmission Control Protocol (TCP).

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Linux Pro	4.3 Monitor and manage system access. • Manage remote connections

CompTIA Linux+	3.2 Given a scenario, configure and implement appropriate access and authentication methods.
	• VPN as a client
	  ◦ SSL/TLS
	  ◦ Transport mode
	  ◦ Tunnel mode
	  ◦ IPSec

	◦ DTLS