	PRO	CON
SSL VPN	› Web browser-based technology provides near-universal access › Supports multiple platforms, including various OSes and devices › Allows better control over access to specific data and applications › Low total cost of ownership	› Users could access the network from an untrusted client › Unless caches are cleaned, agency data could end up on public systems › May require add-on authentication methods beyond user name/password › Some integration needed for legacy client-server applications
IPSec VPN	› Client software ensures strong device authentication › IT can better control which devices can access the network › Better support for enterprise applications, such as VoIP and databases › Easier to enforce other security policies, such as virus control, on remote systems	› Can be expensive to deploy and manage › Requires IT to configure all client devices › Users can only access the network from machines with client software › Firewalls and network address translation can hinder access