

IPsec (Internet Protocol Security) is a framework for a set of [protocols](#) for security at the network or [packet](#) processing layer of network communication.

Download this free guide



## Download Your Guide to the ISACA CISM Certification

Take a closer look at the ISACA Certified Information Security Manager certification, including the value it provides security professionals, how it compares to other security professionals, and what the CSX program offers

Start Download

Earlier security approaches have inserted security at the [Application](#) layer of the communications model. IPsec is said to be especially useful for implementing [virtual private networks](#) and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Cisco has been a leader in proposing IPsec as a standard (or combination of standards and technologies) and has included support for it in its network [routers](#).

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both [authentication](#) of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.