IP Security

Prof Brijendra Singh
Department of Computer Science, Lucknow University, Lucknow

Internet Protocol Security (IPsec)
is a secure network protocol
suite that authenticates and encrypts the packets of data
to provide secure encrypted communication between
two computers over an Internet Protocol network. It is
used in virtual private networks (VPNs).

The IP security architecture (IPsec) provides cryptographic protection for IP datagrams in IPv4 and IPv6 network packets.

This protection can include confidentiality, strong integrity of the data, data authentication, and partial sequence integrity.

IPsec provides security mechanisms that include secure datagram authentication and encryption mechanisms within IP.

A security association contains the following information:

- Material for keys for encryption and authentication
- The algorithms that can be used
- The identities of the endpoints
- Other parameters that are used by the system

IPsec provides two mechanisms for protecting data:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

- Authentication Headers (AH) provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.

Encapsulating Security Payloads (ESP) provides confidentiality, connectionless data integrity, data-origin authentication, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.