IP Security

IPsec (IP Security) is a framework that helps us to protect IP traffic on the network layer because the IP itself doesn't have any security features at all. It is a suite of protocols developed to ensure the integrity, confidentiality and authentication of data communications over the IP network. It is independent of specific encryption algorithms and can support several cryptographic methods(AES, DES). It is supported on both IPv4 and IPv6 platforms.

The IPSec consists of 2 main protocols:

1. **The Authentication Header (AH) protocol**

It is a header in an IP packet, which contains a cryptographic checksum for the contents of the packet. It provides authentication, integrity and an optional anti-replay service to IP.

2. **The Encapsulating Security Payload (ESP) protocol**

It is based on symmetric key cryptographic techniques and can be used in isolation and or it can be combined with AH. It provides confidentiality and integrity of messages.

Working of IPSec

IPSec can work in two modes:

1. Transport mode:

In this mode, IPSec encrypts traffic between two hosts. There will be encryption only for the data packet and not the IP header.

2. Tunnel mode:

In this mode, IPSec creates virtual tunnels between two subnets. This mode encrypts the data as well as the IP header and is thus mostly preferred.

Benefits of IPSec

IPSec is used:

1. To encrypt application layer data.

2. To provide security for routers sending routing data across the public internet.
3. To provide authentication without encryption, like to authenticate that the data originates from a known sender.
4. To protect network data by setting up circuits using IPsec tunneling in which all data is being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Disadvantages of IPSec

1. **Wide access range.**

Since IPSec provides wide access range, it has higher chances of giving privileges to other devices in the network.

2. Compatibility Issues:

There are a couple of compatibility issues with software that happens when software developers do not adhere to the standards of IPSec.

3. CPU Overhead:

It requires quite a bit of processing power to encrypt and decrypt all the data that passes through the server.

Application ofIPSec

1. Secure Remote Internet Access:

We can make a local call to our Internet Service Provider (ISP) to connect to our organization's network in a secure manner. This enables us to access the corporate network facilities or access remote desktops/servers.

2. Secure Branch Office Connectivity:

Rather than subscribing to an expensive leased line for connecting its branches across cities/countries, an organization can set up an IPSec-enabled network to securely connect all its branches over the Internet.

3. Set Up Communication with Other Organizations

IPSec can also be used to connect the networks of differentorganizations together in a secure and inexpensive manner.

Virtual Private Network (VPN)

A VPN is a mechanism of employing encryption, authentication and integrity protection so that we can use a public network (such as the Internet), as if it is a private network such as a physical network created and controlled by you).

VPN combines the advantages of public network (cheap and easily available) with those of a private network (secure and reliable).

Working of VPN

Data is transmitted from your client machine to a point in your VPN network. The VPN point encrypts your data and sends it through the internet. Another point in your VPN network decrypts your data and sends it to the appropriate internet resource, such as a web server, an email server, or your company's intranet. Then the internet resource sends data back to a point in your VPN network, where it gets encrypted. That encrypted data is sent through the internet to another point in your VPN network, which decrypts the data and sends it back to your client machine.

Benefits of VPN

1. It ensures security by providing an encrypted tunnel between a client and VPN server.
2. It can be used to bypass many blocked sites.
3. It facilitates anonymous browsing by hiding your IP address.
4. Also most appropriate Search engine optimization (SEO) is done by analyzing the data from VPN providers which provide country wise stats of browsing a particular product. This method of SEO is used widely my many internet marketing managers to form new strategies.

Disadvantages of VPN

1. **Slow Connection Speeds**

Creating and maintaining the VPN will take a certain amount of bandwidth, which slows connection speeds.

2. **VPN Blocking Software Exists**

Some e-Commerce sites utilize software, which works to identify and prevent users from using VPNs.

3. **Complicated Set Up**

Failing to set up the VPN correctly can result in leaks. Information leaks can occur when using a VPN that is not correctly configured.

4. **Dropped Connections**

A dropped connection over VPN means that your true network information is now on display for anyone.