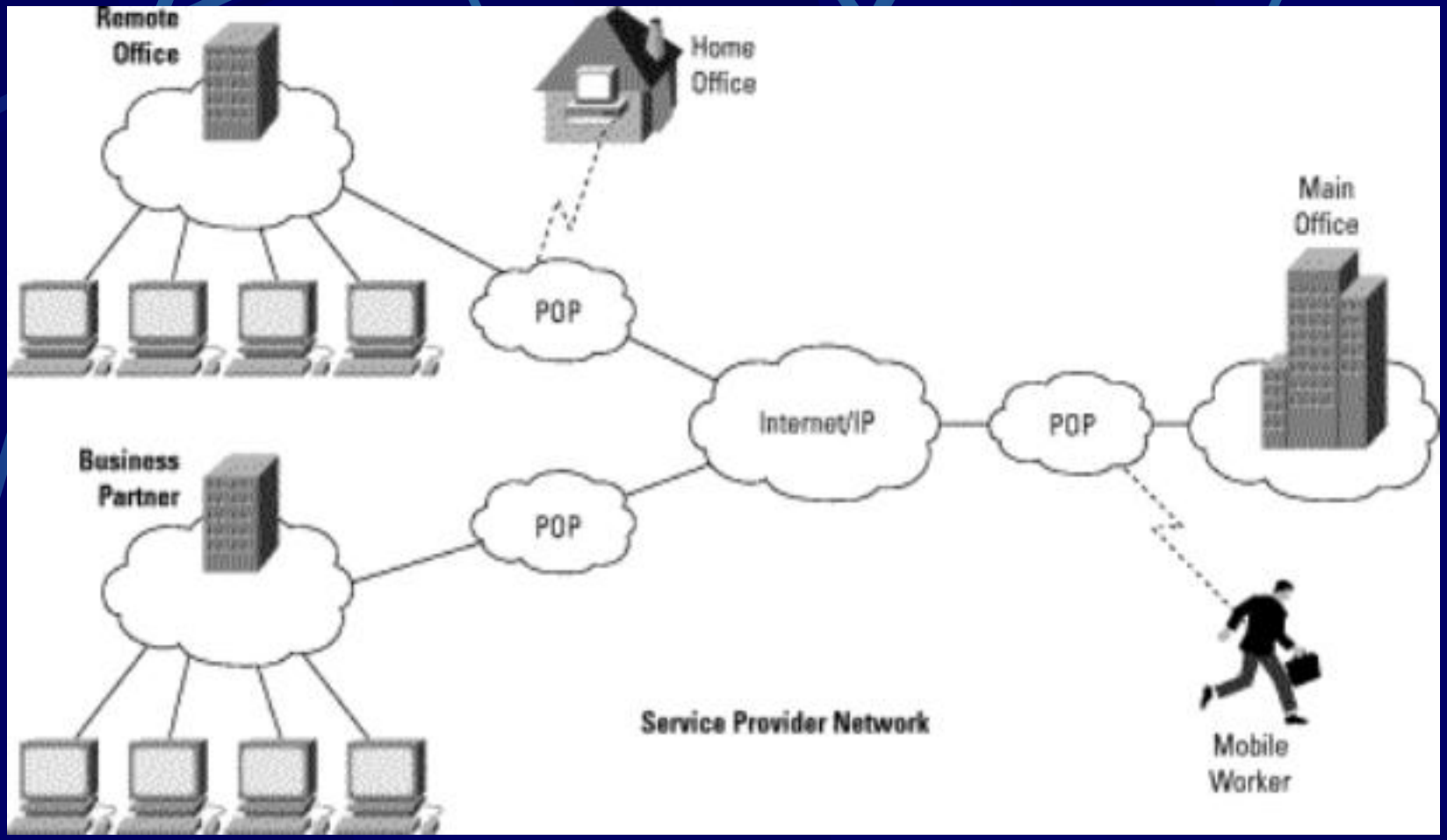
Virtual Private Network

By Ashish Inkar

Virtual Private Network (VPN)

- VPNs are private data networks over public network – usually the Internet.
- VPNs extend corporate networks to remote offices, mobile users, telecommuters and other extranet partners.
- VPNs use advanced encryption and ‘tunneling’ technology to establish secure, end-to-end private network connections over Internet.

A typical VPN



VPN Solutions

Remote access VPNs establish secure, encrypted connections between mobile or remote users and their corporate networks via a third-party network, such as a Internet Service Provider(ISP)

- VPN client – software, hardware as well as router, or firewall based solutions available.
- Reduced cost of long distance access calls and internal equipment inventory

VPN Solutions

Site-to-Site VPNs are an alternative WAN infrastructure that used to connect branch offices, home offices, or business partners' sites to all or portions of a company's network.

- Intranet VPNs provide full access to company’s network
- Extranet VPNS provide business partners with limited access to a company’s network

VPN Technology

- *Trusted VPNs* – companies lease circuits from communication providers and use them in the same manner they use physical cables in a private LAN

- Communication provider is '*trusted*' for data integrity and security.

- Used before Internet became universal

VPN Technology

- *Secure VPNs* use Internet as a corporate communication medium. Data is encrypted before sending, moved over to Internet, and then decrypted at the receiving end.

- Encryption creates a security ‘tunnel’ that can’t be attacked
- More desirable than Trusted VPNs

VPN Technology

- *Hybrid VPNs* – A secure VPN is created as part of the trusted VPN thus creating a ‘hybrid’ VPN. Secure part of the VPN is usually administered by customer (using VPN equipments).
- Secure VPNs that are administered by ISPs are called *provider-provisioned VPNs*.

VPN Building Blocks

- *Security* is built around authentication, authorization, and accounting capabilities.
- Network, data, and addresses are encrypted so they are understood by right sender and receiver only.

VPN Building Blocks

- *Quality of Service* addresses two fundamental requirements – predictable performance and policy implementation
- QoS capabilities allow users to prioritize service classes, manage bandwidth, and avoid congestion.
- Pkt. classification based on IP address, TCP/UDP port no, IP precedence(3bits in the ToS field of IP header), MAC address, URLs & sub-URLs

VPN Building Blocks

- *Management* of devices – ‘simpler is better’
  - Element-based – less expensive. adequate for managing & monitoring small setup
  - Policy-based – centralized for larger networks, policies established and push them to all applicable devices
- Outsource VPN management to the ISP or SASP

VPN Building Blocks

- VPNs provide reliable access to network
- VPN software allows transmitted data packets to transparently switch over to a different path in case of a device failure
- Redundancy in hardware components reduces the risk of downtime

VPN Gateways

- VPN gateways can be categorized as Standalone or Integrated.
- *Standalone* VPNs incorporate purpose-built devices between - the source of data and WAN link *OR* between the modem and a data source in a remote office.
- Integrated implementations add VPN functionality to existing devices such as routers, firewalls.

Gateway Solutions

- Router based VPNs – adding encryption support to existing router(s) can keep the upgrade costs of VPN low.
- Firewall based VPNs – workable solution for small networks with low traffic volume.
- Software based VPNs – good solution for better understanding a VPN, software runs on existing servers and share resources with them

Gateway Solutions

- Internet Security Devices – Standalone VPN devices specifically designed for tunneling, encryption, authentication are easier to setup and make attractive choice for business looking for ‘turn key’ solutions

Outsourcing

Things to consider before outsourcing -

- For connecting remote offices consider an ISP that also offers POP to connect to Internet as a local call
- Redundancy of equipment, connections, and people
- Provider policies, equipment, employee qualification to deal with outside hackers and viruses
- On-site consulting assistance

VPN Protocols

- IPSec – Internet standard protocol for tunneling. Encryption, and authentication.
- Layer2Tunneling Protocol (L2TP) – Provides a means for tunneling IP traffic in layer 2, encloses non-Internet protocols i.e. IPX, SNA, and AppleTalk inside IP envelope.
- Point-to-Point tunneling - proprietary Microsoft

Benefits of using VPN

- Lower costs – remote access costs have reduced by 80 percent while LAN-to-LAN connectivity costs is reduced by 20-40 percent. For companies just setting up their network VPN provides low-cost alternative to backbone equipment, in-house terminal equipment and access modems.
- Connectivity Improvements – VPN based links are easy and inexpensive ways to meet changing business demands.

Benefits of VPN

- Anywhere anytime access – ubiquitous public internet offers transparent access to central corporate systems i.e. email, directories, internal-external web-sites.

VPN technology is improving rapidly and promises a bright future for data communication, its cost-effective, and high returns on investment will outweigh any skittishness in investing in new technology.