



MOBILE IP VPN CONNECTIVEY AND SECURITY



Mobile IP VPN Connectivity

1. Objective

This document describes a short overview of VPN technology and specifies the standards and processes used. VPN is one part (but only part) of securing a mobile and distributed network.

2. Introduction

A virtual private network (VPN) is a group of computers connected to a private network (a network built and maintained by an enterprise solely for its own use with limited public-network access), that communicates "securely" over a public network.

Data VPNs typically have been implemented at the data link layer using Frame Relay and ATM networking technologies for roughly ten years. Now, VPN services based on IP and the use of the Internet are quickly gaining public interest and market acceptance. Like traditional VPNs, IP VPNs utilize shared facilities to emulate private networks and deliver reliable, secure services to end users. Mobile IP VPNs, which provide these services over wireless media, also use IP tunneling technologies.

The business benefits of deploying Mobile VPNs (MVPNs) are numerous.

- Mobile IP VPNs can help companies reap benefits such as dramatically lowered WAN costs, improved global connectivity, and better reliability, while enabling capabilities such as secure extranet communications.
- MVPNs can provide remote workers with constant connectivity to corporate sites or to the ISPs and ASPs of their choice.
- MVPNs also enable businesses and ISPs to outsource mobile access
- By enabling always on connectivity, Real time information can be shared.

3. Implementing Mobile VPNs

Various types of VPN connectivity implementations are possible depending on the business needs of the contracting enterprise. These connections can be lumped as: gateway-to-gateway, gateway-to-host, host-to-gateway, and host-to-host.

Various protocols can be used to implement MVPN: IP Security (IPSec) protocols, Multi-Protocol Label Switching (MPLS) and L2 Tunneling Protocol (L2TP). IPSec based Firewall's are common and appropriate for most business needs.

IPSec is made up of three main protocols:

- Authentication Header (AH) Protocol provides integrity and authentication to IP packets.
- Encapsulating Security Payload (ESP) protocol is used to provide encryption for IP data.
- Internet Key Exchange (IKE) Protocol is used for all IPSec negotiations.

IPSec is typically used in one of the two modes: gateway-to-gateway or host-to-gateway. Refer to Figure1, figure 2 for those MVPN implementations. Gateway-to-gateway connection is the preferred MVPN implementation because host-to-gateway end-to-end connection contain important weaknesses:

- Mobile must support IPSec client
- IPSec will use up to 30% of airlink bandwidth
- NAT (Network Address Translation) is not available

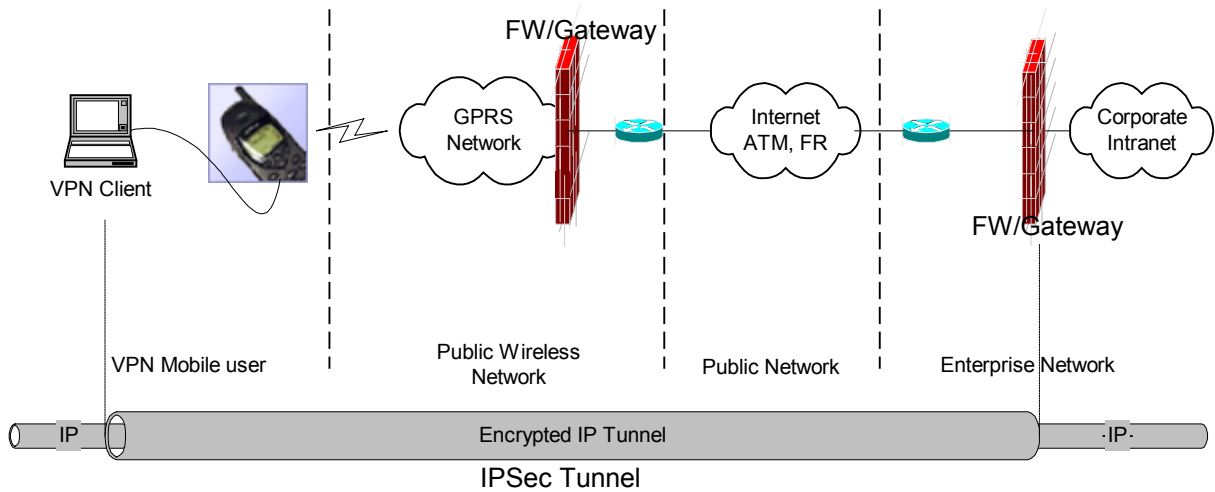


Fig.1 VPN -- Host-to-Gateway connection

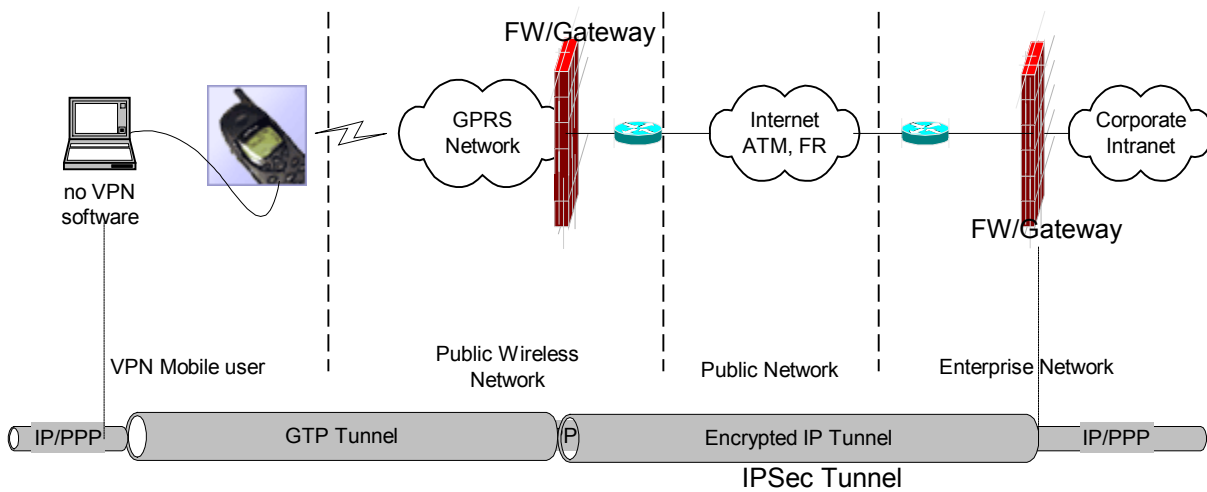


Fig.2 VPN -- Gateway-to-Gateway Connection

MVPN access is provided through one of two access modes in GPRS – Transparent or Non-Transparent. GPRS transparent access mode is intended to provide only IP-based communication and creation of IP-type Packet Data Protocol (PDP) context at GGSN.

With Transparent GPRS access mode:

- GPRS operators offer connectivity to IP network without any user authentication
- Mobile devices do not send any authentication request at PDP context activation
- GPRS operators issue public addresses to GPRS users

The host-to-gateway VPN connection is the only solution in GPRS transparent access mode. The transparent access mode needs more airlink bandwidth, more public IP addresses and IPsec supported mobile devices.

A wireless GPRS network is already deployed with non-transparent GPRS access:

- The MS is dynamically allocated a private IP address.
- GGSNs request user RADIUS authentication based on user authentication requests made at PDP context activation.
- Tunneling IPSec protocols are used between GGSN and ISPs to transmit user traffic to a final destination point, such as: corporate private network.

In non-transparent access service operation, the GPRS network needs to assign APN network identifiers to corporations. The APNs are used by the SGSN to select the GGSN to be addressed for a specific group of corporate mobile users and are also used for billing. The GGSN determines the IP addresses of the GGSNs to which mobile users will be attached.

Unique APNs for large corporations allow an additional level of authentication to the corporate customer as it allows a unique access profile for the customer to be implemented in RADIUS.

The MVPN system architecture is shown in Figure 3.

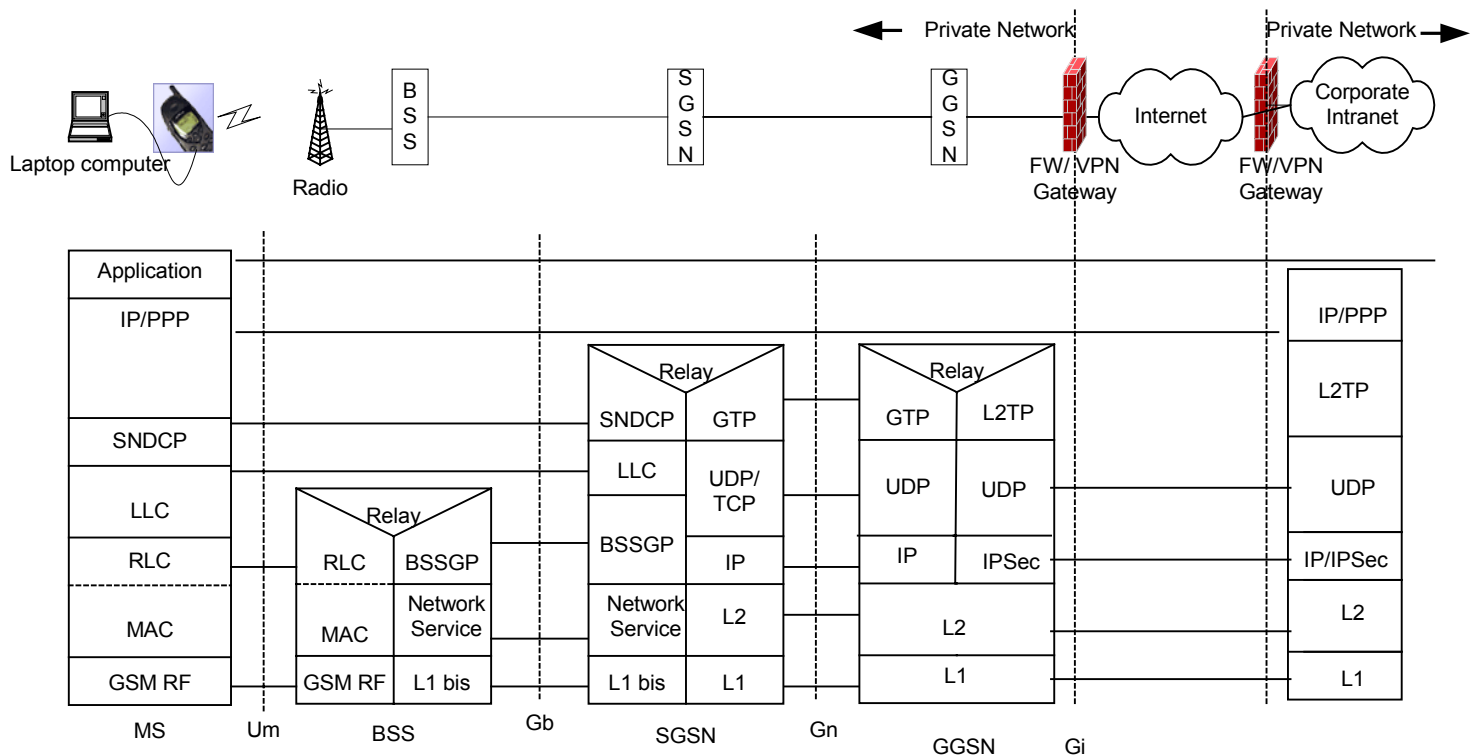


Fig3. GPRS Non-Transparent Access, IPSec-Based VPN

4. Mobile VPN Gateway and Capacity

There are many choices to build a VPN to link corporate networks. In theory, all of the IPSec-based VNP gateways are compatible with standard VPN-1 gateways. Nevertheless, extensive testing is required to determine the extent of this compatible.

VPN concentrators are implemented at Toronto, Montreal and Vancouver to ensure that sufficient capacity is available and operational requirements are met.

A typical standard VPN implementation from major carriers would include:

- IPsec-Based supported
- Authentication Header: MD5 (Message-Digest Algorithm)
- Encapsulating Security Payload: 3DES(triple Data Encryption Standard)
- Internet Key Exchange: Diffie-Hellman
- No Integrated Certificate Authority (CA)
- Interface: 10- or 100-Mbit/s Ethernet through Internet
- Concurrent connections: 50+

5. Conclusion

VPN technology is an important part of an overall secure solution for protecting data within a mobile, wireless or distributed network. However VPN technology is not by itself sufficient to ensure a secure operation. Each layer of the OSI stack must be protected and secure. VPN technology is sufficient in many cases to protect the data link layer and transfer of data but it should be augmented with other technologies. The following grid provides a simple overview of technologies in securing a mobile architecture:

Layer 7 Application	x.400, Programs that use the Network	SSID (hardware to access points)
Layer 6 Presentation	SNMP, FTP, Functions apps need	Extensible Authentication Protocol, Access Lists, SSL, SHTTP
Layer 5 Session	Protocol software which handles functionality	Wireless Equivalency Protocol
Layer 4 Transport	TCP, UDP, end to end, sce and dest hosts	Proprietary Token Card, Certificates
Layer 3 Network	IP. Host/Network Communication	Mobile IP, ICMP, IPSEC, VPN
Layer 2 Data Link	HDLC, Frames between host and packet switches	PPP, 802.1x, VPN
Layer 1 Physical	Interconnection host and network	802.11b, VPN

While VPN's provide speed, and secure access in joining nodes on disparate networks, they are only one piece of the greater security puzzle. Most major Telco carriers provide M-VPN access and services and care should be taken by clients to understand how M-VPNs fit into an overarching security architecture.

If you have any questions please call 416-259-3343 or email us at info@m-trilogix.com

m-trilogix Ltd. 47 Jutland Rd., Etobicoke, M8Z 2G6