Virtual Private Networks over the Internet

Manuel Günter (mguenter@iam.unibe.ch)

August 3, 1998

Abstract

This working paper is a surveys of current activities in the development of solutions for virtual private networks over the Internet. The paper is related to the CATI project (WP2T1 and WP2T2) which is founded by the Swiss National Foundation.

1 Introduction

The essence of a virtual private network (VPN) is a temporary, secure connection over a public network. In this paper we are interested in IP-VPNs. These are virtual private networks using the Internet as public network. In order to save growing telecommunication costs, companies recently started to replace expensive leased lines and dial-up remote access by IP-VPN solutions which are cheaper, because they only use a local link to the company's Internet service provider (ISP). A further advantage of IP-VPN solutions is the global reach of the Internet. Some IP-VPN solutions even claim to be more secure than the traditional telecommunication approaches.

The main goal of companies adapting IP-VPN solutions is to minimize telecommunication costs. A 1997 VPN Research Report by Infonetics Research Inc. estimates savings from 20% to 47% of wide area network costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs [IBM98].

Many companies are currently evaluating the deployment of a VPN over the Internet. According to a 1997 Forrester survey, more than half of the 50 fortune 1000 companies interviewed said within two years they expected to use the Internet to communicate with partners. Two-thirds said they intend to execute transactions with customers over the Internet [Ave98a].

A vast variety of VPN solution vendors target the new market. ISPs provide solutions to their customers, while hardware vendors (e.g. Cisco and IBM) and Software vendors (Microsoft, Shiva, Aventail, 3com) sell solutions to the companies and ISPs as well. The bigger vendors also try to establish their own standards. This is not surprising, since the VPN market is expected to reach at least several billion dollars by the year 2001 [Ave98b]. IDC and Link Research forecast that VPNs will continue to grow at an annual rate of 45 percent through 1999 [Ave98a].

In the rest of this paper we will discuss what the advantage and disadvantages of IP-VPNS are, what different VPN types there are and what protocols they use. Then we conclude.

2 Pros and Cons of IP-VPNs

VPNs as well as the traditional telecommunication approaches are aimed to boost productivity by *extending the reach of the companies resources*. This includes hardware (computers, LANs) electronic services (file service, database access) as well as human resources (voice mail).

In order to extend the reach of a company's Intranet(s) a VPN over the Internet promises two benefits: *cost efficiency* and *global reachability*. However there are three major concerns about VPN technology: security, managability and performance.

Security. In order for Virtual Private Networks to be private the transmitted data must be encrypted before entering the Internet, since the Internet is considered an untrusted network. Everybody can connect to the Internet and there is no guaranty that participants stick to any policy or rule. However, protecting the traveling data will not protect the information inside the Intranet from unauthorized access. Therefore, more elaborate VPN architectures must include additional protection such as firewalls and user authentication mechanisms.

Managability. The companies telecommunication requirements and equipments evolve at a high speed. The VPN management must be able to cope with these changes avoiding high expenses. VPNs are connected to many different entities that even by themselves are hard to manage and that constantly evolve. Such entities include the companies physical network (eventually featuring unregistered IP addresses), the companies security policy, the companies electronic services, the companies ISP(s) to mention but a few. The VPN solution vendor Cisco considers the managability of VPNs to be the key to profitably deploying VPN service [Sag98].

Performance. Since ISPs deliver IP packets still on a "best effort" basis, the transport performance of a VPN over the Internet cannot be predicted, it is variable. Current research is focusing on easing this situation [FBH98]. Furthermore, security measures (encryption and authentication) can decrease transport performance significantly. This also points out two management problems: The clients must be enabled to (1) measure the performance and (2) customize the VPN (e.g. the security options) in order to optimize it [BS97].

3 Different Types of VPN Solutions

We differ between two main types of VPN solutions: the ones that target an ISP who wants to offer VPN services and the ones that target a company who wants to use a VPN.

Products for ISPs (like offered by Cisco) usually include software for the ISP's customer, too. Such products are more extensive since they manage several VPNs, the ISP's physical network and they provide charging and accounting facilities. In this model, ISP clients outsource most of the VPN management and only manage the IP services they want to offer over their VPN.

"Big" IT companies that also act as ISPs (IBM, Microsoft) use their own solutions on their networks and try to sell VPN hard- and software to their Internet service customers. Microsoft's VPN security choice PPTP (point-to-point tunneling protocol) which is embedded in Windows NT v4.0 is even free.

"Small" VPN solution vendors (e.g. Shiva) try to sell provider independent products. Advantages of such approaches are improved security (data is protected from the ISP), company internal network equipment optimization, reduced dependence (protection from changes at the ISP) and reduced time-to-deployment. These client side solutions often use open standards (IPsec, ISAKMP, Socks v.5) and are open for the use of different protocols (e.g. encryption with DES, IDEA, etc). Provider independent VPN solutions come with the inconvenience of having to manage the VPN and its client software as well as additional hardware (tunnel terminating device). Furthermore, there is no mean of monitoring and configuration of the transport performance outside of the own Intranet.

3.1 Different VPNs for Different Purpose

Beside of the overall benefits of VPNs a company may want to use VPNs for different kinds of tasks which require different solutions. Here are the three most common scenarios [IBM98, Ave98b]:

Remote access network. A remote user that is at home or on the road needs access to his/her company's electronic resources. An ideal VPN enables the remote user to work as if (s)he was at a workstation in the office. Authentication, transparency and ease of use for the remote user are crucial factors for this scenario.

Branch office connection network. Here, two or more trusted Intranets are connected. Usually the Intranets are protected by firewalls which are the ideal location to deploy VPN software. Thus, the client workstations do not have to worry about the VPN. Problems arise from managing unregistered (private) IP addresses and shielded DNS entries [Mos97b], managing access rights and possibly from transport performance.

Business partner/supplier networks. This scenario (also called Extranet) represents the most recent trend for VPN usage and also the least mature field. Companies can grant their partners temporal and limited access to their Intranet. The wide availability of the Internet and its relatively small costs together with mature IP-VPN technology shall allow fully functional e-business applications including initial contact of customer, sales negotiation, order fulfillment and ongoing support. Furthermore such a solution allows to automate the supply chain and facilitate collaborative projects with partners [Ave98a].

However, Extranet are exposed to the most severe management problems of the three kinds of VPNs. It is the fast pace of evolution and the dynamics of interacting with partners that cause problems in the following areas: security (e.g. key management), fine grained access control (company wide access policies needed), consistency and possibly charging and accounting.

4 VPN Protocols

We said that "private" in "Virtual Private Network" means encryption and authentication but what about "virtual"? A network is virtual when a protocol makes a physically discontinuous system appear as *one network* to the higher protocols. Note that it seems to be the first choice to place such a VPN protocol at the lower layers in the ISO-OSI reference model, namely at the data link layer and the network layer. However, as we will see, higher protocol layers can be an option, too.

4.1 VPN Protocols in the OSI Reference Model

Here is a list of the common VPN protocols starting from OSI layer 2 (data link) along with the protocols' key features.

Point-to-Point Tunneling Protocol (PPTP). Microsoft extended the ubiquitous Point-to-Point Protocol (PPP) by running it as the inner protocol with the Generic Routing Encapsulation (GRE) protocol (RFC 1701, 1702). PPTP emerged of Microsoft's client/server-LAN experience. Thus it uses the Remote Access Services (RAS) of the client for user authentication.

PPTP is limited in usage. It offers remote connections to a single point. It does not support multiple connections nor does it easily support network-to-network connections. PPTP's security is

also limited. It does not offer protection from substitution- or playback attacks, nor does it provide perfect forward secrecy. PPTP has no clear mechanism for renegotiation if connectivity to the server is lost [Mos97a].

Level 2 Tunneling Protocol (L2TP). This protocol also guides PPP over an IP network, but is a simpler version of GRE. L2TP came out of the router-ISP-engineering community. Thus it uses the Remote Authentication Dial-In User Service (RADIUS) at the ISP. L2TP is similar to PPTP and they both target the remote access scenario. L2TP delegates security features toward IP Security (IPsec) which we present next. Beside of that it suffers from the same drawbacks as PPTP [Mos97a].

Internet Protocol Security (IPsec). IPsec evolved from the IPv6 movement and is promoted as a standard by the IETF. It is located in OSI-layer 3. IPsec is a broad-based open solution for encryption and authentication on a per-packet basis. IPsec can securely encapsulate IPv4 packets and tunnel them from one firewall to another. Thus it is an optimum solution for trusted LAN-to-LAN VPNs (the branch office connection network scenario presented in section 3). IPsec can ensure authentication, privacy and data integrity. It is open to a wide variety of encryption mechanisms. IPsec is application transparent and a natural IP extension, thus ensuring interoperability among VPNs over the Internet. Router vendors and VPN hardware vendors support IPsec. Commercial implementations start to be introduced to the market in 1998.

Nevertheless, there are disadvantages of IPsec. IPsec is bound to the TCP/IP stack[1]. IP addressing is part of IPsec's authentication algorithm. This is less secure than higher layered approaches and it is a problem in dynamic address environments which are common to ISPs. IPsec requires a public key infrastructure which is still subject to current research. IPsec does not specify a methodology for access control beyond simple packet filtering. Furthermore, IPsec's development is delayed by ongoing IETF committee infighting and is not explicitly supported by Microsoft [Ave98b].

SOCKS v5 and SSL. SOCKS v5 was originally approved by the IETF as a standard protocol for authenticated firewall traversal. When combined with the Secure Socket Layer (SSL) it provides the foundation for building highly secure VPNs that are compatible with any firewall. SOCKS v5 strength is access control.

SOCKS v5 controls the flow of data at the session layer (OSI-layer 5). It establishes a circuit between a client and a host on a session-by-session basis. Thus it can provide more detailed access control than protocols in the lower layers without the need to reconfigure each application. SOCKS v5 and SSL can interoperate on top of IPv4, IPsec, PPTP, L2TP or any other lower level VPN protocol. A session layer solution does not have to interfere with the networking transport components, thus the clients are non-intrusive. SOCKS v5 provides plug-and-play capabilities including access control, protocol filtering, content filtering, traffic monitoring, reporting and administration applications.

On the minus side, SOCKS v5 decreases performance. Also, client software is required to build a connection through the firewall to transmit all TCP/IP data through the proxy server [Ave98b].

The discussion of these three protocols indicates what VPN purpose (see section 3.1) their are best used for. The result is shown in the following table. An architecture is sketched in figure 1

[1] Since here we are dealing with IP-VPNs the limitation to TCP/IP is not a real disadvantage.

VPN type	Protocol	OSI Layer
Branch office connection network	IPsec	1 and 3
Basic remote access	PPTP, L2TP	2
Secure remote access	SOCKS v5 and SSL	5 (ev. 3)
Business partner networks	SOCKS v5 and SSL	5 (ev. 3)

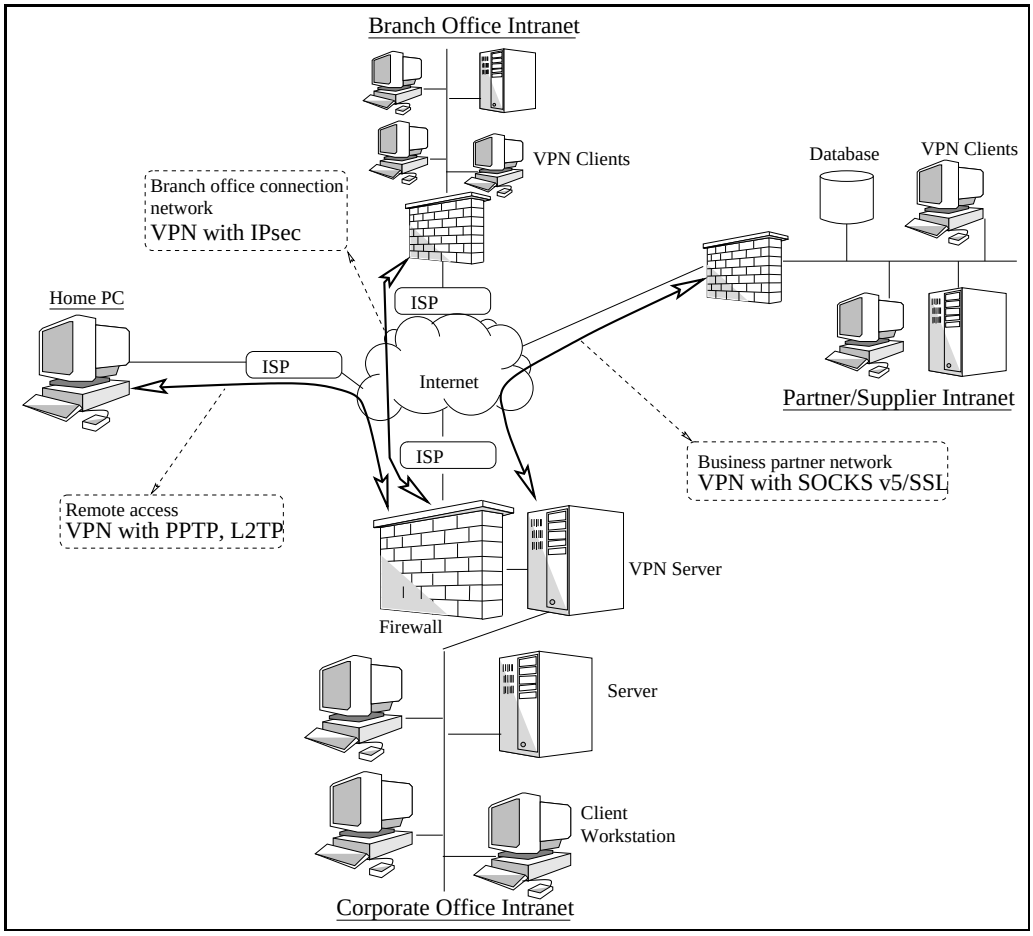

Figure 1: Client based VPN scenarios.

The four presented VPN protocols operate at the borders of the Internet. However, there are also VPN protocols for Internet backbone routers.

4.2 VPN Backbone Protocols

As mentioned in section 3 network hardware vendors like Cisco offer VPN solutions that target ISPs. The solutions enable the ISPs to configure their network in order to offer diversified services to their customers. This includes quality of service and availability guarantees which the Internet cannot give. Therefore, solutions proposed by Cisco [Sag98] or Ericsson [HW98] implement the Multiprotocol Label Switching (MPLS) technology for the ISP's backbone routers. MPLS forwards IP packets over an ATM network. It is being standardized by the IETF.

Multiprotocol Label Switching MPLS is deployed in a ISP's IP backbone network that uses IP routers at the edges of the network and ATM switches controlled by a MPLS component in the inside. The basic idea is to do (intelligent) layer 3 routing at the edges of the backbone network and to do fast layer 2 forwarding inside the backbone network. Incoming IP packets get a MPLS header attached, they are labeled according to IP header information (mainly the target address, but also type of service and other fields). A label switched path is set up for each route or path through the network. Once this is done, all subsequent nodes may simply forward the packet along the label-switched path identified by the label at the front of the packet. Negotiations of labels between nodes is done by the label-distribution protocol of MPLS. An ATM connection is set up for each label-switched path. Thus, MPLS can support quality of service. MPLS makes the underlying backbone infrastructure invisible to the layer 3 mechanisms. This light-weighted tunneling provides an extendible foundation that provides VPN and other service capabilities. Furthermore, the MPLS architecture enables network operators to define *explicit* routes. Note that there is ongoing research on multicast functions in order to improve the scalability of MPLS.

MPLS technologies are useful for ISPs that want to offer their customers a wide band of IP services. The ISPs add value to their service e.g. by offering the complete management of the customers VPN. Obviously, the more the customers outsource their VPN management, the more crucial network management becomes to the ISP. The OSI reference model does not support network management. Therefore, for example Cisco bases its IP-VPN solution on the ITU's Telecommunication Management Network (TMN) reference model.

The Telecommunication Management Network Reference Model. Figure 2 shows the five layer hierarchy of the model as presented in [Sag98]. The *element layer* covers embedded technologies

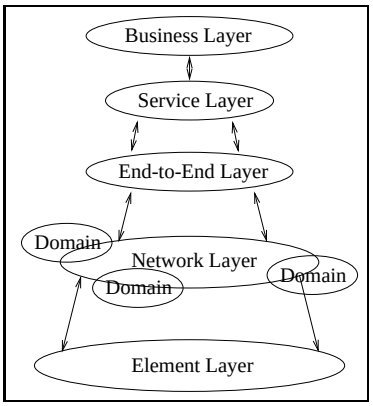

Figure 2: The TMN Five-Layer Model

that manage the individual element (router, gateway etc.) to monitor performance and detect faults. The *network layer controls* the elements on a device-by-device or domain basis. The *end-to-end layer* connects the domains together to provide an integrated view across different equipment and protocol types. The *service layer* supports the management of services and service-to-service interaction. Finally, the *business layer* supports the driving of the customer relationship, such as sales, ordering, and billing, in addition to customer reporting and other customer network management applications.

5 Summary

In todays global market the availability of the companies electronic resources to the authorized personnel, customers and partners is believed to be a major competitive factor. However, remote dial-up and leased lines are expensive. Many companies therefore evaluate the deployment of virtual private networks over the Internet. Such solutions are price-effective and have a wide reach. Problems of such IP-VPNs are security, managability and performance. For the simple VPN scenarios (remote access and trusted LAN-to-LAN networks) good protocols and solution exists and are in use. Nevertheless, there are still topics that need future work:

- In the security area the IETF working group is still arguing over scalable key distribution solutions.
- Managing methodologies and tools for more complicated VPNs (Extranet scenario) with a company wide security policy and fine grained resource access control are still incomplete or missing.
- ISPs offering diversified services (e.g. outsourced VPN) not only have to manage their network, but they must charge and account the use of their service and allow their customers to control or even configure their VPN transport performance.
- Finally scalable quality-of-service solutions for the Internet remain a research topic.

References

[Ave98a] Aventail. Extranet VPNs: Paving the way for e-business. http://www.aventail.com/educate/whitepaper/extranetwp.html, 1998.

[Ave98b] Aventail. Making sense of virtual private networks. http://www.aventail.com/educate/whitepaper/vpnmarketwp.html, 1998.

[BS97] Gordon Burnes and Greg Stoller. Virtual private networking: The next revolution in corporate productivity. http://www.shiva.com/remote/prodinfo/vpn/index.html, 1997.

[FBH98] T. Braun F. Baumgartner and P. Habegger. Differentiated services: A new approach for quality of service in the internet. Working paper, 1998.

[HW98] Boran Hagard and Mikael Wolf. Multiprotocol label switching in ATM networks. *The Telecommunications Technoloty Journal*, 1998.

[IBM98] IBM. eNetworks VPNs - IBM's virtual private networks solutions. http://www.software.ibm.com/enetwork/library/whitepapers/white_vpn.html, 1998.

[Mos97a] Robert Moskowitz. Take a hard look at virtual private networks. http://intranetsolutions.3com.com/articles-new/look/, 1997.

[Mos97b] Robert Moskowitz. Virtual private networks: Harder than you think. http://intranetsolutions.3com.com/articles-new/think/, 1997.

[Sag98] Karen M. Sage. Network management solutions for IP-VPN service. http://www.cisco.com/warp/public/779/servpro/solutions/csm/vpn_wp.htm, 1998.