Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 79 (2001)

Heft: 1

Artikel: Means to support distributed and enterprise internal communication needs

Autor: Stiller, Burkhard

DOI: https://doi.org/10.5169/seals-876510

Virtual Private Networks

Means to Support Distributed and Enterprise internal Communication Needs

Virtual Private Networks (VPN) show an important technology choice to allow for the solution of the interconnection of remotely distributed, enterprise internal subnetworks, as well as of the remote access problem for company employees. While traditional VPNs are based on Frame Relay or Asynchronous Transfer Mode technology, the Internet Protocol (IP)-based Internet offers highly economic alternatives for the setup of so-called IP VPNs. IP VPNs combine the advantage of the packet-based, public Internet – e.g. its inherent flexibility of providing varying bandwidth requirements – with enterprises' demands on privacy, secured data transmission, and Quality-of-Service (QoS).

BURKHARD STILLER

Communication between people and between enterprises, the exchange of news, information, and data has changed in the last few years dramatically. While data communications in the 70's and 80's required dedicated networks and links to interconnect highly important computers and sites, communications have become widespread and globally accessible with the emerging triumphal procession of the Internet and its inherent protocol of the network layer, the Internet Protocol (IP). Although the World Wide Web, electronic mail, telnet, and various additional applications have been targeted at the single user and his support initially, company networks based on IP are equally important for today's enterprises and commercial business scenarios. So-called Intranets define enterprise internal networks for various purposes, ranging from administration and backup networks to production and information-sharing backbones. Exactly at this point two orthogonal requirements have to be taken care of:

- the Internet's public and open characteristic, available to everyone, and
- enterprises' legal demand to share a public networking infrastructure, but keep private company internal communications crossing the public network.

The need for enterprises to allow their highly mobile and laptop-carrying employees universal and worldwide access to corporate data and information anywhere, anytime, at any speed, and at a defined quality becomes another relevant business critical issue of an up-to-date communication infrastructure. This drives the additional demand to enlarge Intranets with remote access possibilities, which are economically maintainable and operable. As shown below, leased lines are in many cases not an economically viable networking approach any more, large modem pools for remote access are not an economic solution, either.

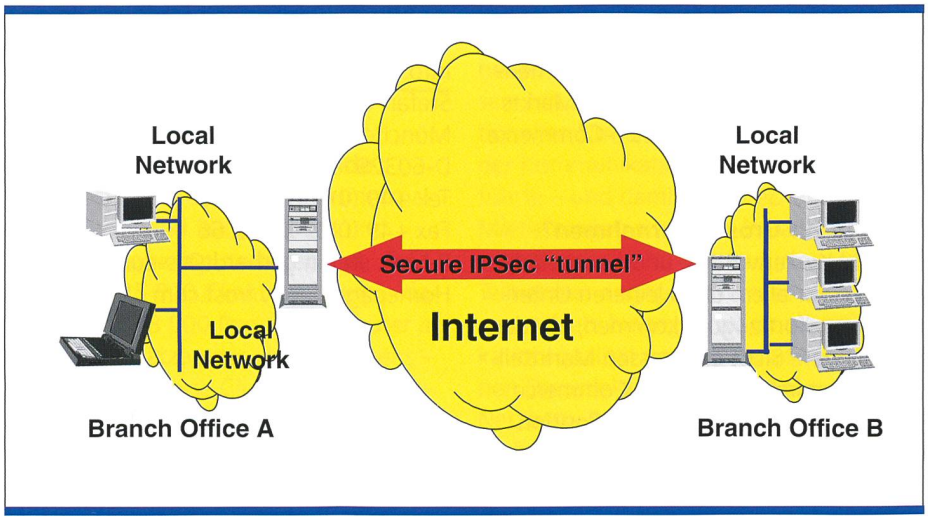

Fig. 1. Intranet VPN-based on a Compulsory IPSec Tunnel.

History, Definition, and VPN Types

Traditionally, company networks have been built on top of leased lines and dedicated communication links. With respect to existing networking technology choices, such as X.25, Frame Relay, or the Asynchronous Transfer Mode (ATM), these systems have been utilised to implement the long-distance network to interconnect distributed enterprise subnetworks. Drawbacks of these interconnection solutions include (a) high investment costs for leased lines, (b) the inherent difficulty to determine in advance an exact bandwidth demand for these lines and the consequence of highly varying utilisation figures, (c) a lengthy administration process for setting them up, and (d) a potential lack of communication security.

While restricting the point of view at this stage to the Internet, drawbacks (a) and (b) do not exist, since the access to the Internet is less expensive than leasing links, and the packet-based nature of IP communications offers variable bit rate services. With respect to drawback (c), recent advances in VPN management systems, such as described in [3], have provided solutions for flexible IP-based VPN technology. Finally, the developments of an Internet security architecture (IPSec) [4] and appropriate protocols and components define an excellent step for overcoming drawback (d).

Based on these aspects and as described in [1], a Virtual Private Network (VPN) defines a private network, which has been configured and setup across a pub-

licly accessible networking infrastructure. In particular, an IP VPN determines a VPN running on top of the Internet Protocol (IP) and related protocols, developed by the Internet Engineering Task Force (IETF). Typically, an IP VPN, VPN in short for the reminder of this paper, employs some combination of encryption, digital certificates, strong user authentication, and access control, while more recently Quality-of-Service (QoS) support has been added in support of further business-critical applications [3].
In general, four classes of VPNs are distinguished: (1) link-layer, (2) network-layer, (3) transport-layer, or (4) application-layer VPNs. For the second class, and in particular IP VPNs, three types are differentiated, there are (1) an Intranet VPN, which determines an enterprise network and regular access control functionality, (2) an Extranet VPN, which combines multiple enterprise and customer networks and an appropriate access control scheme, and (3) an Access or Dial-up VPN, which offers the functionality of remote access to enterprise data via service provider Points-of-Presence (PoP). Non-IP VPNs encompass a link-layer model, which is similar to a conventional private data network, a Multiprotocol Over ATM (MPOA) model using an encapsulation mechanism, and Multiprotocol Label Switching (MPLS) model applying dedicated labels within a single routing domain [2].

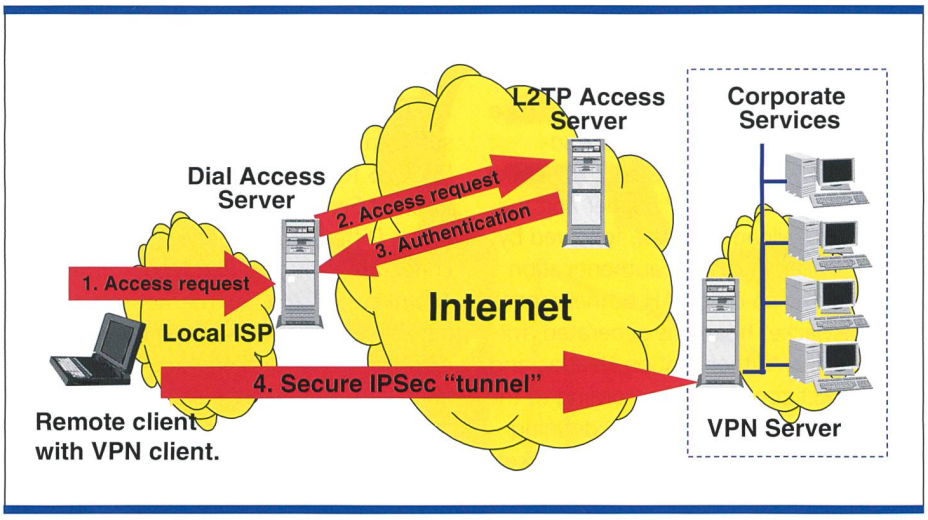

Fig. 2. Dial-up VPN-based on a Voluntary IPSec Tunnel.

IP VPNs

Virtual Private Networks based on the Internet Protocol (IP VPN) provide Intranet and Extranet solutions for enterprises with remotely distributed subnetworks. The underlying Internet provides routing, packet forwarding, and packet transmission tasks, without the need to configure explicit paths, such as for Frame Relay or ATM VPNs, which results in similar LAN (Local Area Network) and WAN (Wide Area Network) communication technology. Any type of IP VPN can be viewed by users as an Intranet, although traffic is transparently transported across the public Internet. While the public backbone's IP protocol is extended to the enterprises' domain, basically only communication endpoints from the Internet's perspective need to be configured. Two alternative choices exist: (1) the Internet access provider locates an IP edge router within the enterprise's domain, which outsources the enterprise's networking responsibilities to the provider, or (2) the Internet access provider interconnects privately-owned IP edge routers and allows for an enterprise inhouse networking responsibility. These choices offer a range of diverse policies in edge routers and, in particular, provide the platform for various security policies to be implemented.

VPN Tunnelling

To bridge remote subnetworks transparently, a packet encapsulation or tunnelling scheme is applied in IP edge routers belonging to the same Intranet. This tunnel may be constructed voluntarily, i.e. on purpose for a specific user request, e.g., for Dial-up VPNs, or it may be constructed compulsorily, e.g. without any user interaction, but during the VPN configuration time. In the latter case, every IP packet originating within an Intranet utilises private VPN IP addresses, which are not known to the public Internet, and they are embedded into new IP packets, which are constructed in IP edge routers and which carry publicly known IP addresses. While the IP source address of this exterior IP packet corresponds to the public IP edge router's address of the originating VPN site, the new IP source address of the exterior IP packet will be set to the public destination address of the other VPN site. These two public edge router's IP addresses define the two tunnel endpoints of the VPN tunnel. The most common tunnelling schemes defined today include the Generic Routing Encapsulation protocol (GRE), the Distance Vector Multicast Routing Protocol (DVMRP), the Point-to-Point Tunnelling Protocol (PPTP), and the Layer 2 Tunnelling Protocol (L2TP). PPTP defines a combination of the Point-to-point Protocol (PPP) and IP, where standard PPP dial-up frames are encapsulated in IP. PPP includes an authenticated dial-up standard with a 128 bit encryption. L2TP combines PPTP and the Layer 2 Forwarding (L2F) to establish the two tunnel endpoints in a compulsory fashion, i.e. without any user interaction. Figure 1 depicts a situation where two branch offices are interconnected by a compulsory tunnel. In this case the tunnel is secured particularly by applying the IPSec protocol [4].
In case of a Dial-up VPN a dial-up client performs an access request (fig. 2) to a Dial Access Server (or Network Access Server), which in turn forwards this request to a L2TP Access Server (or a RADIUS server) to authorise the request for accessing corporate services within the destination VPN. Once the authentication is granted, the remote client – determining a remote VPN client – will establish the secure tunnel to the VPN server within the corporate network.

Security Protocols

As shown above, the tunnelling mechanism establishes a communication relation between two remote VPN sites or between a dial-up client and his "home", the corporate network. However, this tunnelling by itself will be not sufficient, as the applied IPSec protocol already suggests. While tunnelling allows for the utilisation of private, VPN-internal IP addresses for clients connected to the VPN, IPSec ensures that IP packets being transmitted over this tunnel are secured [4].

IPSec defines an Authentication Header (AH), as well as an Encapsulation Security Payload (ESP), which are added in different ways to the original IP packet. In case of pure encryption purposes, the so-called ESP transport mode, an ESP header will follow the original IP header and the encrypted payload is added, followed by the ESP trailer. In case of authentication purposes, the so-called AH tunnel mode, a new IP packet header is generated, followed by the Authentication Header, and an IP packet constructed according to the ESP transport modus is added, defining the "new" payload of the new IP packet. It has to be noted that AH and ESP are independent of a particular encryption algorithm, such as symmetric encryption based on 3DES, IDEA, or Blowfish, or asymmetric encryption based on RSA or ElGamal. Therefore, an initial setup is required to define the applied algorithms as well as the particular keying material in use. This task is performed by an Internet Key Exchange (IKE) protocol, which allows for manual as well automated key exchanges and X.509 certificates.
These security mechanisms are applicable to VPNs, in particular, the ESP transport mode can be configured at IP edge routers of figure 1, to ensure that traffic crossing the tunnel is always encrypted. Due to the fact that encryption is performance critical, the edge router (or a dedicated firewall) relieves single VPN clients from this task and maintains necessary keying material for the entire VPN site. Of course, this scenario allows for a site-to-site encryption only, where traffic inside the VPN site is accessible to all VPN clients. In case of a dial-up VPN it has to be ensured that the remote client is authorised to access the VPN.
Therefore, the AH tunnel mode is applicable to establish a tunnel (fig. 2), while the data transfer afterwards may follow the ESP transport mode.

Agreements between Customers and Providers based on Quality-of-Service

Service Level Agreements (SLA) define the service level to be maintained between customers and providers. With respect to VPNs, an SLA may be negotiated to establish the security level in case of the outsourced scenario as well as the QoS level. While the content and technical level of specification of SLAs for the Internet are still issues of debate, charging-relevant information needs to be part of future contracts based on SLAs as well [5]. However, various bandwidth and QoS requirements can be supported by VPNs, if the underlying IP technology provides sufficient functionality. As described in [3], QoS for VPNs can be supported by an Internet Service Provider (ISP), if he operates a Differentiated Services Internet Architecture including Bandwidth Brokers. A broker hierarchy of internet service brokers for a single networking domain and external service brokers for inter-ISP enables SLA negotiations and the configuration of IP edge routers according to specific customer VPN QoS demands. Within this approach, fully automated and customer-driven VPN service establishment is possible by configuring tunnel endpoints over a Web interface, including the specification of bandwidth demands and security requirements.

Conclusions

Today, IP VPNs are an economic and technically viable solution to set up large Intranets and Extranets, which virtualises services and segregates communications to closed user groups and enterprises. While the IP tunnelling mechanism allows for point-to-multipoint IP packet transmission, the IPSec-based encryption and authentication ensures secured data transmission. In addition, the reduction of higher costs, mainly for leased lines, is a second driving factor for VPNs by tak-

References

[1] P. Ferguson, G. Huston: What is a VPN? – Part I; The Internet Protocol Journal, Vol. 1, No. 1, June 1998, pp 2–19.

[2] P. Ferguson, G. Huston: What is a VPN? – Part II; The Internet Protocol Journal, Vol. 1, No. 2, September 1998, pp 2–18.

[3] M. Günter, I. Khalil, T. Braun: An Architecture for Managing QoS-enabled VPNs over the Internet; 24th IEEE Annual Conference on Local Area Networks, LCN'99, Lowell, Massachusetts, U.S.A., October 18–20, 1999, pp 122–131.

[4] S. Kent, R. Atkinson: Security Architecture for the Internet Protocol; Request for Comments, IETF, RFC 2401, November 1998.

[5] B. Stiller, T. Braun, M. Günter, B. Plattner: The CATI Project: Charging and Accounting Technology for the Internet; 5th European Conference on Multimedia Applications, Services, and Techniques (ECMAST'99), Madrid, Spain, May 26–28, 1999, LNCS, Springer Verlag, Heidelberg, Vol. 1629, pp 281–296.

Glossar

Dial-up VPN:	A Dial-up VPN is a form of an Intranet, which additionally allows for the access of corporate services from a mobile client via a Point-of-Presence (POP) and an authentication server.
Intranet:	An Intranet defines a particular form of a VPN, which shows some longer term established tunnels between remote enterprise sites.
IPSec:	Internet Security Architecture, which defines different modes for the encryption and authentication of IP traffic.
IP VPN:	An Internet Protocol (IP)-based Virtual Private Network defines a VPN on top of Internet technology.
SLA:	A Service Level Agreement (SLA) defines, in the case of the Internet, Quality-of-Service (QoS) requirements as well as further parameters for a service delivery contract established between two parties, mainly the enterprise (customer) and a network provider.
Tunnelling:	Tunnelling describes a mechanism to encapsulate IP packets into new IP packets to ease its handling in public networking infrastructure, mainly IP routers.
VPN:	A Virtual Private Network (VPN) defines a private network, which has been configured and setup across a publicly accessible networking infrastructure.

ing advantage of the economies of scale for the public Internet and its application as a shared communication platform. However, since IPSec protocols and components are not completed fully, most importantly the IKE remains incomplete, practical VPN solutions lack a certain degree of interoperability, if available networking equipment from different vendors is to be used. Therefore, careful investigation of heterogeneous infrastructures is required, in case it needs to be prepared for an IP VPN. This includes the evaluation of technology with respect to its particular functionality, e.g. VPN configuration support, IPSec, QoS support, firewall tasks, or any combination of those.

The outsourcing alternative as discussed above, where IP edge routers belong to the provider, shows a major disadvantage of outsourcing trust to the provider as well, since the IKE as well as the keying material applied are located in the domain of the provider. Provider-independent, in-house IP edge routers permit site-to-site tunnelling and security as well as the integration of dial-up clients. Furthermore, every single client could be equipped with keying material to establish enterprise-internal security domains. However, this approach requires the installation of a VPN server, sometimes called VPN gateway as well, at each and every site to enable remote dial-up clients, including VPN client software, to access a particular VPN. In addition, the policy and security management of VPNs requires an essential portion of technology expertise and business knowledge. Only its close cooperation and the definition of common goals will enable the VPN to be successful.

Concluding, Internet protocol-based Virtual Private Networks in general are promising with improved scalability for dial-up clients, customer-driven provisioning, rapid service creation, and configurable security policy support. However, the range of fully interoperable products and their implementation of complete IETF protocols still lies ahead.

9.4, 10

Burkhard Stiller, *Computer Engineering and Networks Laboratory TIK, Swiss Federal Institute of Technology, ETH Zürich, Switzerland, E-Mail: stiller@tik.ee.ethz.ch*

Zusammenfassung

Private Netze

Virtuelle Private Netze (VPN) stellen die Lösung für das Netzwerkproblem dar, möglichst kostengünstig die Kopplung einer Kommunikationsinfrastruktur verschiedener Firmenstandorte über ein öffentliches Netzwerk zu erlauben. Während traditionelle VPNs zum Beispiel auf der Frame Relay Technologie oder dem Asynchronen Transfer Modus (ATM) basieren, bieten Internet Protokoll (IP)-basierte VPNs (IP-VPN) eine flexiblere und ökonomische Alternative. Sie kombinieren die Vorteile des paketbasierten, öffentlichen Internets mit den Firmenanforderungen an private, sichere und dienstgüteorientierte Kommunikation. Ein VPN wird somit im Allgemeinen als ein privates Netzwerk definiert, welches auf einer öffentlich zugänglichen und gemeinsam genutzten Netzwerkinfrastruktur für spezielle Firmenbedürfnisse konfiguriert wurde.

IP-VPNs werden zur Realisierung von firmeneigenen Internets oder Extranets verwendet und erlauben die Nutzung einer identischen Weitverkehrs- und lokalen Technologie, eben der IP-Technologie. In diesem Zusammenhang werden die öffentlichen Netzwerkkomponenten und -funktionen «mitbenutzt», um einen privaten Kommunikationskanal, einen so genannten Tunnel, einzurichten, der die Firmenstandorte verbindet. Diese Funktionen umfassen sowohl die Routing-Funktionalität wie auch das Paket-Forwarding sowie die IP-Paketübertragungen. Hierbei ist es möglich, die Endpunkte eines oder mehrerer Tunnels am öffentlichen Internetzugang zu konfigurieren und den VPN-internen Endsystemen ein geschlossenes Netzwerk, eben ein virtuelles Netzwerk, anzubieten. Diese VPNs können vordefinierte Tunnels aufweisen, aber auch über Anwählklienten (Dial-up) erreicht werden, die sich an einem Point-of-Presence (PoP) in das öffentliche Internet einwählen und dann über einen Authorisierungs-Server eine Zulassung erhalten.

Es existieren eine Vielzahl von Tunnelprotokollen, wie das Generic Routing Encapsulation Protocol (GRE), das Distance Vector Multicast Routing Protocol (DVMRP), das Point-to-Point Tunnelling Protocol (PPTP) und das Layer 2 Tunnelling Protocol (L2TP). Während das PPTP eine Kombination aus dem Point-to-Point Protocol (PPP) und IP darstellt, kombiniert L2TP das PPTP weiter mit dem Layer 2 Forwarding (L2F), um die Tunneleinrichtung zu erlauben. Wesentliche Unterschiede bestehen schliesslich im Einsatz von Verschlüsselungs- und Sicherheitsprotokollen, die den Datentransfer auf einem VPN sichern. Die Internet Sicherheitsarchitektur IPSec definiert zwei verschiedene Arten von Moden. Im Encapsulation Security Payload (ESP) Transportmodus werden IP-Pakete in verschlüsselter Form in neue IP-Pakete eingebettet und mit einem zusätzlichen ESP Paketkopf versehen. Im Authentication Header (AH) Tunnelmodus wird ein mittels ESP Transportmodus gesichertes Paket mit einem AH versehen, um eine Standort-zu-Standort Authentifizierung zu erlauben. Während IPSec in dieser Form keine speziellen kryptographischen Algorithmen vorschreibt, ist die Internet Key Exchange (IKE) dafür verantwortlich, das Schlüsselmaterial für die Algorithmen bereitzustellen und zu verwalten. Schliesslich basieren die Dienstgüten (Quality-of-Service, QoS) einer VPN-Dienstleistung auf den Vereinbarungen zwischen VPN-Anbieter und Firma auf den Service Level Agreements (SLA). Diese legen unter anderem fest, welche QoS ein VPN und seine Tunnels aufweisen müssen.

IP-VPNs zeigen eine kostengünstige und effiziente Möglichkeit, private Netze auf der Basis des öffentlichen Internets zu realisieren. Die vorhandenen Technologien der verschiedenen Hersteller zeigen jedoch eine grosse Bandbreite an speziellen und nicht unbedingt immer kompatiblen Funktionalitäten und Protokollen. Aus diesem Grunde ist es wesentlich, beim Aufbau eines VPNs und der Auswahl der notwendigen lokalen Infrastruktur, wie den Zugangs-Routern, eine exakte Funktionsprüfung und einen Protokollinteroperabilitätstest vorzunehmen.