Virtual Private Networks

Crescenzio Gallo
Department of Clinical and Experimental Medicine, University of Foggia, Italy

Michelangelo De Bonis
University of Foggia, Italy

Michele Perilli
University of Foggia, Italy

INTRODUCTION

Within technologies for the safe use of interconnected computer systems, Virtual Private Networks (VPNs) represent a segment with a remarkable development both from the commercial (both in the private sector and the public administration) and the technological side, where we see significant investments by vendors and system integrators. All these involve rapid and interesting innovations in the proliferation of advanced services by specialized operators and, in general, in the growth of this sector.

A VPN (Connolly, 2002; Golen, 2002; Tyson, 2008) enables you to separate different types of traffic and implement secure private connections across public networks through labeling techniques, tunneling and traffic encryption (Browne, 2001; Cisco Systems, 1999). VPNs are an effective and safe way to extend services, applications and enterprise networks, beyond the physical boundaries of individual organizations by transparently supporting the innovative services of today's network infrastructures. Development supported by the investments from the main protagonists of networking (satisfying functionality, manageability, scalability, and security) has led to a gradual improvement in the functionality of encryption techniques, authentication sessions, tunneling and traffic engineering. To these basic functionalities, we can add other features such as the support for Voice and Video applications over IPSec VPNs (Cisco Systems, 2002), or the possibility of configuring multi-point VPNs by dynamically adding and/or removing nodes.

Today it is possible to administer, from a single management point, the deployment and configuration of tens of thousands of VPNs, centrally administer the security policies for each user, and remotely set the configurations of the various hardware and software devices, making it also extremely simple and transparent to network users (Awad et al., 2013). All these are elements that describe the two main strands on which the further development of VPN technologies is also based: support for advanced converged networks (data, voice, video, storage on a single IP network infrastructure), and simplifying the implementation of such systems.

BACKGROUND

VPN Safeness

A Virtual Private Network is a special way to create secure and confidential connections between two or more geographically distant nodes (PCs, networks, mobile devices) by allowing data to travel over a public TCP/IP (e.g. Internet) network, as a result of the encoding of all the traffic from one point to another. Before VPNs companies used "dedicated" lines, a really expensive kind of solution. By exploiting the Internet, it is possible to establish a sort of independent and autonomous "lane" between the company and its branches at low cost. This particular technique is called "tunneling".

A VPN can be implemented starting from selecting only some nodes to build a new private network characterized by its arbitrary size and transparency to network users, which are not aware of the underlying physical infrastructure. Contrary to previous technologies, the problem of IP security is no longer faced by a physical point of view (Gollmann, 2006). Historically, the public infrastructure prevented unauthorized users from physically send data to other people's VPNs

DOI: 10.4018/978-1-4666-5888-2.ch624

ensuring isolation without other special additional means. But the IP protocol is not capable of physical isolation, and then it prepares a series of "logical" mechanisms (authentication, encryption) capable of simulating "physical" security.

Because a VPN host could be an Internet node, the belonging of a packet to the VPN will be controlled through certain protocols ensuring that only data from "trusted" sources could be processed. In other words, rather than blocking the arrival of data from "outside", you prevent their forwarding onto the private network through appropriate mechanisms of mutual recognition among the VPN members.

What are the main problems that a security system must address to ensure the reliability of a VPN?

- **Reservedness:** The ability to keep a confidential communication. On unsecured communication links a hacker, through simple techniques, can be able to capture (and display) all traffic flowing between any hosts. The effects on the confidentiality of communications are harmful. It would be easy to get hold of sensitive information such as credit card numbers and passwords.
- **Integrity:** The ability to ensure that in a communication data will be delivered to the recipient exactly as sent by the transmitter. This property prevents the communication to be changed without the knowledge by the two end-points.
- **Authentication:** The ability to make sure of the identity of the other party. Identity theft, or pretending to be someone else, is always very dangerous. In an electronic transaction you have very few means to verify the correct identity of the other party.

These features can be exploited to the maximum degree through *digital signature*, which employs asymmetric cryptography (by means of public and private keys) to ensure reservedness, integrity and authentication (together with non-repudiation).

Another problem is the definition and respect of an appropriate quality of service (QoS) in VPN communications (Sandick et al., 1998). Unlike previous networks, where bandwidth-delay parameters were often guaranteed from the physical infrastructure, IP gives milder warranties, especially in the presence of VPNs spanning multiple operators.

VPN RESERVEDNESS

Tunneling protocols are used by clients and servers to manage the VPN tunnel and send the information in protected mode. The following section provides descriptions of the most commonly used protocols.

GRE (Generic Routing Encapsulation)

The GRE protocol (Hanks, 1994) specifies a generic encapsulation mechanism for the transport of any protocol. It provides that the original packet is encapsulated with a GRE header, and then encapsulated in the protocol (typically IP) that will be responsible for transporting it to the destination. The GRE header includes a Protocol Type field, with the same encoding used for Ethernet, which indicates the transported protocol. In turn, GRE responds to the IP Protocol Type (code 47). There are no specific authentication mechanisms and thus it is possible to exploit IPSec.

PPTP (Point-to-Point Tunneling Protocol).

PPTP (Eisinger, 2001) is a network protocol enabling secure data transfer from a remote node to a server through a virtual private circuit built on a TCP/IP network such as the Internet. The IP packet is encapsulated in a PPTP header, and PPTP is responsible for maintaining the confidentiality of the virtual channel by encrypting data in transit. Once connected, you can employ commonly used protocols as IP, IPX, and NetBEUI to access resources on the local network. This eliminates the need for long-distance calls or a costly dedicated network. PPTP is a standard proposed by companies such as Microsoft, Ascend Communications, 3Com USR Robotics and is supported by different operating systems, for both the client and the server.