

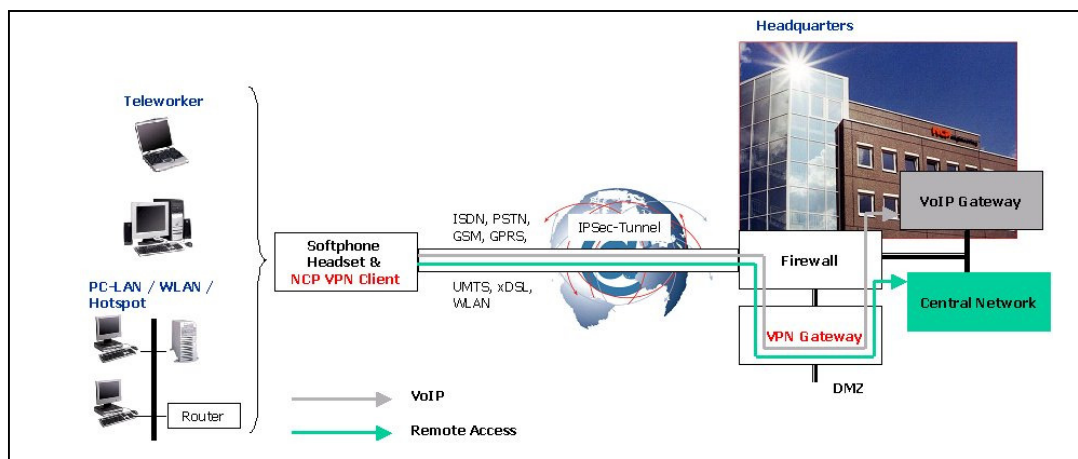
LANline August 2006

Page 40 / 41

Security and Quality of Service Voice over IPsec Infrastructures

Today, many companies are standing before the task of total communications processes, and therefore also developing the language in an IP-based company-wide data network (intranet) via the internet. When it involves voice-over IP, security and quality of service (QoS) are the central themes.

Since technology and quality of VoIP solutions have been improving steadily in recent years and has become user friendly, defective security in the internet now qualifies as the brake-block to the introduction of VoIP. While conventional publicly switched telephone networks (PSTN), a conversation is transmitted in a dedicated channel from end to end over a copper cable, benefits of Voice-over IP media, for which many users have concomitant access. This presents the same security problems compared to public IP-based networks, LANs and WLANs (hotspots) with which users already are confronted remote access/mobile computing. VoIP transforms analog speaking signals for transmission in the internet into digital data packets, providing it with a unique sender and target address – the so called IP address – and finally transmits it over the internet to the receiver. Here, the digital data packets are again transformed into analog spoken data. As a rule, since speech data packets today are unencrypted underway, the danger exists that hackers would attain access.



Virtual Private Network (VPN) with Voice- and Dataintegration


There are already freely obtainable tools that transform unencrypted recorded spoken data packets and transform them into an audio format. Tools that enable an attacker to obtain unauthorized access to the computer of a VoIP user are likewise sufficiently well known. Further imaginable are backdoor attacks on company networks in connection with remote

access applications. By the way, the same exposure underlies the data for connection control, since these are likewise transmitted unencrypted. It should be strictly determined, that each present and also future form of attack that is based on internet protocol and that threatens data networks is transferable on VoIP. Therefore, with internet telephone engineering, the same security measures must be grasped as with typical long-distance data transmission. Practice has demonstrated that singular security precautions do not suffice. Only the combination of different security mechanisms guarantees comprehensive protection from each and any attack on the terminal and the company network. In today's situation however, there no comprehensive security solutions for VoIP on the side of manufacturers of VoIP-TK equipment and also providers.

VoIP Security rely on VPN technology

A practical security solution is already available with the tunnelling technology in a virtual private network (VPN). The associated catchwords are called VoIPSec (Voice over IPsec) or VoVPN (Voice over VPN) in the intranet. On the basis of efficient data encryption, companies can secure their VoIP infrastructure sustainably internally and externally against attacks. With the IPsec-based VPN solution, all data packets are securely transmitted end-to-end between the communications participants. The deciding significance is the manner in which the IPsec protocol on the side of the manufacturer has been implemented into the VPN client-software. All applications – also those for “internet telephone engineering” – must be transparently available for the user. By the way, this does not apply for SSL-VPNs, since these don't support VoIP. A general problem with data transmission via internet, is that the individual data packets typically do not arrive in the correct sequence at the receiver. If data are lost underway, they are reworked until, for example, a complete website has completely loaded.

These time delays have no noticeable effects for the user, for example, while surfing. However, the principle with VoIP manifests itself as problematic. Namely, if some data packets arrive at the receiver too late or not at all, this leads immediately to a noticeable deterioration in conversation quality, somewhat in the form of delay by several seconds (“latency”) or snippets of conversation. Fluctuations in the length of delay (jitter) has a particularly disadvantageous affect. Whoever wants to telephone disturbance-free via the internet, requires a certain “quality of service” level. The basic requirement for this, that VoIP data are granted a higher degree of transmission priority as other data packets, in order to exclude audio delays. An essential functionality is regards bandwidth management. All measures in wide area networks (WAN) are understood under this, to make each service available an optimal bandwidth. Therefore, this applies for the allocation of a certain available bandwidth under supervision of the quality of service (QoS) and to optimize the stipulated service level agreements (SLA). Corresponding systems are to be positioned at both end points of the IP network by the operator. In the case of a virtual private network, these functions must be appropriated/supported by the client and server components. An additional aspect is “traffic shaping”, the artificial constraints of available band width for regulation of traffic. Here, goal setting is also here to use availably placed band width optimally. Thereby, it concerns the question about which priority the data packets are processed (bandwidth management) and not - as with QoS - how the data packets are handled after being sent on the internet. All these functions are made available through correspondingly optimized VPN clients that are disposed as well over all required security



mechanisms including QoS features: Personal firewall, data encryption, support of certificates, VPN tunneling, bandwidth management and traffic shaping. IPSec protocols must be implemented in such a way that all applications can be used transparently by the teleworker in every communications environment. The PC is then already protected before and during the establishment of a VPN connection into the company network.

Optimized VPN Client as Solution

As soon as VoIP data packets queue with an existing VPN connection, the bandwidth for the running application is reduced, for example, with the NCP client. Simultaneously reduced, the system whose data packet size is to be held as small as possible in order to minimize delays by the voice data packet (this is called heightening of speech quality). After ending the telephone call, the data connection is automatically put back into the original condition, i.e. bandwidth and data packet size is increased. In order for the administration of often worldwide distributed teleworker locations to make it easy for fashioning the VPN operator, central management concerns itself with the required transparency in all operational situations, such as rollout, certificate administration, software updates and endpoint security. For VoIP via the internet, each user concerns himself with the security of its speech data. Next to manufacturer-specific solutions, where there is admittedly little interoperability, the IPSec standard offers, next to strong authentication, also end-to-end encryption for all IP data packets. This integrated approach is independent from the application and makes possible the transparent integration of mobile employees into the company network. The prerequisite is that the VPN client-software disposes over the required security and communications features for quality of service. The VPN infrastructure can be used as a universal platform for all future IP-based communications solutions such as video telephone engineering (video over IP).