

Virtual Private Networking with AVM

VPN with AVM

AVM's VPN solutions offer the missing link: AVM Access Server and NetWAYS/ISDN provide field staff, home offices and remote corporate locations with simple and secure access to the enterprise network. With a VPN, network applications that are deployed in a local corporate network can also be utilized at remote locations. A VPN permits the remote use of all IP-based network applications. Classic network applications such as terminal emulation, database applications, Windows file and printer sharing, e-mail and workflow solutions are used in exactly the same way via a VPN as they are in the local corporate network – typically without any modification. AVM's VPN products provide a cost-effective and secure VPN tunnel through the Internet to the corporate network. The AVM Access Server is installed in corporate headquarters and branch offices, whilst NetWAYS/ISDN is best suited to provide connectivity for stand-alone computers.

The VPN Concept

The key idea behind the concept of a "Virtual Private Network" (VPN) is to utilize the Internet as a cost-effective and speedy alternative to a leased line or dial-up connection in order to access a remote network. Confidential data is transmitted via the Internet and protected from prying with the help of powerful and effective encryption techniques. This is often referred to as a "tunnel" built through the Internet directly to the remote site.

Ease of Use

Ease of use was a key focus during the development process of the AVM VPN solutions. Numerous configuration wizards and an intuitive Windows user interface simplify both the installation and administration of the AVM Access Server and NetWAYS/ISDN. As VPN settings can be exported using encrypted configuration files or e-mail, configuring the remote site is child's play.

Security

Both AVM Access Server and NetWAYS/ISDN utilize the established "IPSec" protocol to set up a VPN tunnel. IPSec is an open VPN standard that is well-known for its security. A variety of encryption techniques can be used in IPSec. In addition to the DES and 3DES methods, AVM also supports the state-of-the-art Advanced Encryption Standard. Keys from 128 bit up to 256 bit guarantee the confidentiality and integrity of data well into the future.

The IP stack developed by AVM is independent of the operating system and provides the corporate network with reliable firewall protection from the Internet. Incoming data is meticulously analyzed and, if necessary, filtered by the AVM Access Server using IP packet filters, Network Address Translation (NAT) and Stateful Packet Inspection. A host of carefully preset parameters ensure a safe and secure default configuration. Known patterns of attack, such as inappropriate TCP parameter configuration, teardrop attacks, ping-of-death packets and many other patterns are identified and blocked.

VPN Connection Costs

Cost-saving is a key benefit of the VPN concept – the Internet connection charge is the only cost incurred by either site, regardless of location. Affordable, fast Internet access is available almost globally using a range of access technologies. With AVM Access Server and NetWAYS/ISDN providing both Internet access and VPN connectivity, the cost-effective Short-Hold function can also be implemented in VPN mode. The Internet connection is dynamically set up and terminated on demand, and the requisite VPN tunnel parameters are automatically renegotiated in the background.

VPN with dynamic IP addresses

Many Internet providers, particularly those that offer access for home offices or branch offices, nowadays provide a dynamic IP address only. Many VPN solutions, however, require a static IP address. This is not the case with the AVM VPN solutions. Even with two dynamic IP addresses, the AVM Access Server and NetWAYS/ISDN are able to set up a VPN, allowing the most cost-effective Internet access method to be chosen. If the Access Server is not continuously connected to the Internet, NetWAYS/ISDN is also able to initiate the Access Server's Internet connection with a short, no-cost ISDN call – needless to say that this occurs automatically when a VPN session is being set up.

Speed

Access technologies such as DSL or GPRS are only suitable for connecting to the Internet – direct dial-up to a corporate network is not possible. As a result, these fast and affordable technologies can only be utilized for remote access by implementing a VPN. Additional payload data compression ensures a considerable increase in data transfer speeds. Using IPComp, payload data is transmitted through the VPN tunnel up to 200% faster than physical transfer speeds normally allow.

Open Standards

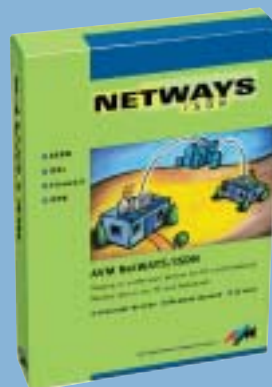
Thanks to extensive support of the IKE and IPsec VPN industry standard protocols, both the AVM Access Server and NetWAYS/ISDN provide total interoperability with a whole host of 3rd party VPN devices.

AVM NetWAYS/ISDN

- Full-featured remote access and VPN client
- Internet connectivity through ISDN dial-up and leased line, DSL, GSM, HSCSD, Ethernet and Microsoft Dial-Up Networking
- IPsec Tunnel Mode
- Authentication Header (AH, RFC 2402)
- Encapsulated Security Payload (ESP, RFC 2406)
- SHA-1, MD5
- DES, 3DES, AES
- IPComp (RFC 2393) with Deflate (RFC 2394), LZS (RFC 3051), LZJH (RFC 2395)
- Internet Key Exchange (IKE, RFC 2490), Main and Aggressive Mode
- Firewall (packet filter, NAT)
- Short Hold Mode, NetBIOS spoofing
- DSL support with AVM FRITZ!Card DSL and Ethernet-DSL modem (PPPoE)
- GSM and HSCSD with FRITZ!GSM

System Requirements

- Minimum: Intel Pentium 200MHz or equivalent CPU
- Windows XP/Me/98 and Windows 2000/NT 4.0
- 64MB RAM



Please note that NetWAYS/ISDN contains additional extensive features that are not related to VPN utilization. Please refer to the separate NetWAYS/ISDN data sheet for further information on these features.

AVM Access Server

- Full-featured VPN Gateway and VPN Concentrator
- Internet connectivity through ISDN dial-up and leased line, DSL, GSM, HSCSD and Ethernet
- IPsec Transport and Tunnel Mode
- Authentication Header (AH, RFC 2402)
- Encapsulated Security Payload (ESP, RFC 2406)
- SHA-1, MD5
- DES, 3DES, AES
- IPComp (RFC 2393) with Deflate (RFC 2394), LZS (RFC 3051), LZJH (RFC 2395)
- Internet Key Exchange (IKE, RFC 2490), Main and Aggressive Mode
- Firewall (packet and port filter, input, output and forwarding)
- Scalable bandwidth using Basic Rate and Primary Rate ISDN Cards
- Authentication with "preshared keys" and X.509 certificates
- Integrated X.509 certification

System Requirements

- Minimum: Intel Pentium 200MHz or equivalent CPU
- Windows 2003, Windows XP, Windows 2000 and Windows NT 4.0 (both Server and Workstation)
- 64MB RAM
- Installation: 50MB free hard-disk space/ Operation (log enabled): up to 250 MB free hard-disk space



Please note that AVM Access Server contains additional extensive features that are not related to VPN utilization. Please refer to the separate AVM Access Server data sheet for further information on these features.

