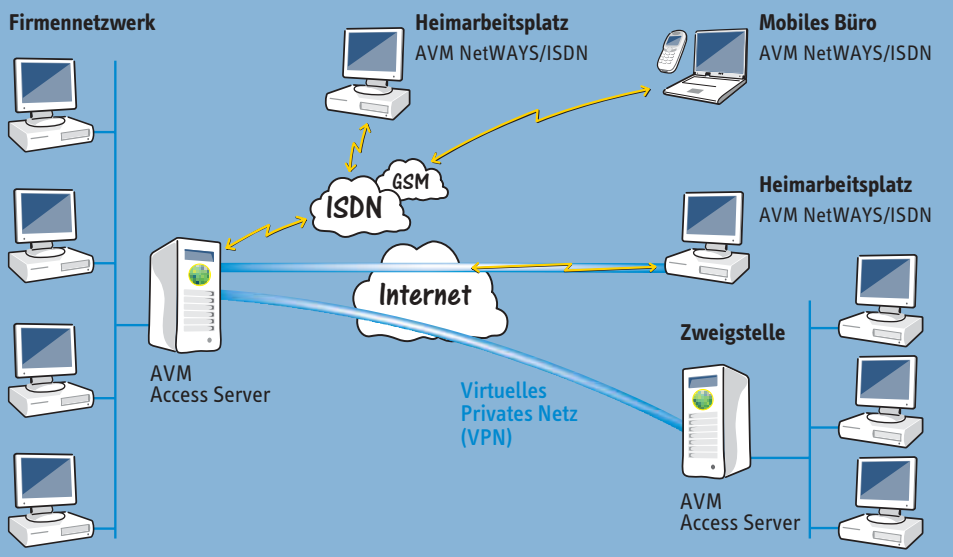


Virtual Private Networking mit AVM

VPN mit AVM

VPN-Lösungen von AVM verbinden, was zusammengehört: Außendienstmitarbeiter, Heimarbeitsplätze und ganze Netzwerke entfernter Firmenstandorte erhalten über den AVM Access Server und NetWAYS/ISDN den sicheren und einfachen Zugang zum Firmennetzwerk. Über VPN können Netzwerkanwendungen, die im Firmennetzwerk zum Einsatz kommen, auch von räumlich entfernten Standorten genutzt werden. VPN ermöglicht die Nutzung aller IP-basierten Netzwerkanwendungen aus der Ferne. Typische Netzwerkanwendungen wie beispielsweise Terminaldienste, Datenbanklösungen, die Windows-Datei- und Druckerfreigabe, E-Mail und Workflow-Lösungen werden über VPN genauso benutzt wie im Firmennetzwerk – in der Regel ohne spezielle Anpassungen. Die VPN-Produkte AVM Access Server und NetWAYS/ISDN bauen hierfür einen kostengünstigen und gesicherten VPN-Tunnel durch das Internet zum Firmennetzwerk auf:
In der Firmenzentrale und in Zweigstellen kommt der AVM Access Server zum Einsatz; für die Anbindung von Einzelplätzen ist NetWAYS/ISDN die richtige Wahl.

VPN – das Konzept

Hinter dem Konzept "Virtual Private Network" (VPN) steckt die Idee, eine Verbindung zum entfernten Netzwerk nicht mehr über eigens angemietete Festverbindungen oder Wählleitungen aufzubauen, sondern stattdessen das Internet als kostengünstiges und schnelles Medium zu verwenden. Die Nutzdaten werden dabei auf ihrem Weg durch das Internet mit Hilfe von leistungsfähigen Verschlüsselungstechniken vor unberechtigtem Abhören geschützt. Man spricht von einem "Tunnel", der durch das Internet zur Gegenstelle aufgebaut wird.

Einfache Bedienung

Die einfache Bedienung der AVM VPN-Lösungen war bereits während der Entwicklung ein wichtiges Ziel. Zahlreiche Assistenten und eine übersichtliche Windows-Oberfläche helfen daher bei der Installation und Administration des AVM Access Servers und NetWAYS/ISDN. Der einfache Export einer VPN-Konfiguration über eine verschlüsselte Datei oder über E-Mail macht die Konfiguration der Gegenstelle zum Kinderspiel.

Sicherheit

Sowohl der AVM Access Server als auch NetWAYS/ISDN bauen den VPN-Tunnel mit Hilfe des etablierten Protkolls IPSec auf. IPSec ist ein offener und weltweit für seine Sicherheit anerkannter VPN-Standard. Innerhalb von IPSec können verschiedene Verschlüsselungstechniken eingesetzt werden. Neben den Verfahren DES und 3DES unterstützt AVM auch den neuen "Advanced Encryption Standard". Mit Schlüssellängen von 128 bis 256 bit wird auch für die Zukunft die Sicherheit vor dem unberechtigten Entschlüsseln der Daten gewährleistet.
Der von AVM selbst entwickelte und vom Betriebssystem unabhängige IP-Stack bietet den zuverlässigen Firewall-Schutz des Firmennetzwerks gegenüber dem Internet. Mit IP-Paketfiltern, Network Address Translation (NAT) und Stateful Packet Inspection werden einkommende Pakete vom AVM Access Server gründlich untersucht und gegebenenfalls gefiltert. Zahlreiche Voreinstellungen helfen, eine sichere Grundkonfiguration zu realisieren. Bekannte Angriffsmuster wie beispielsweise unsinnig gesetzte TCP-Optionen, Teardrop-Attacken, Ping of Death Pakete und viele andere Muster werden erkannt und blockiert.

VPN-Verbindungskosten

Ein großer Vorteil des VPN-Konzeptes ist es, dass unabhängig von der räumlichen Entfernung für beide Standorte nur die Kosten für den Internetzugang anfallen. Günstige und schnelle Internetzugänge existieren heute nahezu weltweit und über verschiedenste Zugangstechniken.
Da der AVM Access Server und NetWAYS/ISDN sowohl den Internetzugang als auch die VPN-Verbindung realisieren, ist der kostensparende Short Hold Mode auch im VPN-Betrieb nutzbar. Die Internetverbindung wird automatisch bei Bedarf auf- und abgebaut, die erforderliche Neuaushandlung des VPN-Tunnels erfolgt automatisch im Hintergrund.

VPN auch zwischen dynamischen IP-Adressen

Viele Internetanbieter, gerade solche, deren Zugänge sich für Home-Offices oder kleine Zweigstellen eignen, bieten heutzutage lediglich eine dynamische IP-Adresse. Viele VPN-Lösungen benötigen jedoch eine statische IP-Adresse. Nicht so die VPN-Lösungen von AVM. Auch zwischen zwei dynamischen IP-Adressen kann mit dem AVM Access Server oder mit NetWAYS/ISDN ein VPN-Tunnel aufgebaut werden, so dass auch kostengünstige Standardzugänge verwendet werden können. Wenn der Access Server nicht ständig mit dem Internet verbunden ist, kann NetWAYS/ISDN sogar über einen kurzen, gebührenfreien ISDN-Anruf die Internetverbindung des Access Servers anstoßen – natürlich automatisch beim VPN-Verbindungsaufbau.

Geschwindigkeit

Einige Internet-Zugangstechniken, wie beispielsweise DSL oder GPRS, eignen sich ausschließlich dazu, eine Verbindung in das Internet aufzubauen. Eine Direkteinwahl ist mit diesen Techniken nicht möglich. Erst mit VPN können diese schnellen und günstigen Zugangstechniken überhaupt für den Fernzugang verwendet werden.
Darüber hinaus ermöglicht die Nutzdatenkompression eine erhebliche Steigerung der Übertragungsgeschwindigkeit. Mit IPComp werden die Nutzdaten mit einer bis zu 200% höheren Geschwindigkeit durch den VPN-Tunnel übertragen als die tatsächliche physikalische Übertragungsgeschwindigkeit.

Offene Standards

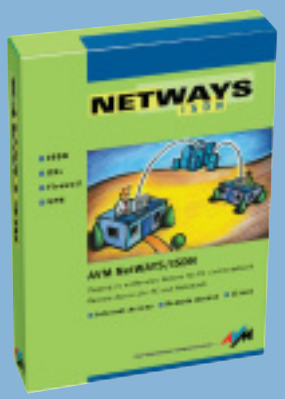
Durch die breite Unterstützung der offenen VPN-Industriestandards IKE und IPSec sind der AVM Access Server und NetWAYS/ISDN zu einer Vielzahl von VPN-Geräten anderer Hersteller interoperabel.

AVM NetWAYS/ISDN

- Umfangreicher Remote Access- und VPN-Client
- Internetanbindung über ISDN-Wähl- und Festverbindung, DSL, GSM, HSCSD, Ethernet, WLAN, DFÜ-Verbindung (für GPRS, UMTS, Analogmodem etc.)
- IPSec Tunnelmode
- Authentication Header (AH, RFC 2402)
- Encapsulated Security Payload (ESP, RFC 2406)
- SHA-1, MD5
- DES, 3DES, AES
- IPComp RFC 2393 mit Deflate (RFC 2394), LZS (RFC 3051), LZJH (RFC 2395)
- Internet Key Exchange (IKE, RFC 2490), Main und Aggressive Mode
- Firewall (Paketfilter, NAT)
- Authentisierung über Preshared Keys oder X.509-Zertifikate
- Smartcard-Unterstützung über Microsoft Cryptographic Service Provider (CSP)
- Short Hold Mode, NetBIOS Spoofing
- DSL-Unterstützung über AVM FRITZ!Card DSL und Ethernet-DSL-Modem (PPPoE)
- GSM und HSCSD mit FRITZ!GSM

Systemvoraussetzungen

- Ab Intel Pentium 200 oder vergleichbarem Prozessor
- Windows XP/Me/98 und Windows 2000/NT 4.0
- Für VPN-Verbindungen über das DFÜ-Netzwerk oder bei Verwendung von Smartcards zur Authentisierung: Windows XP, 2000
- 64 MB RAM



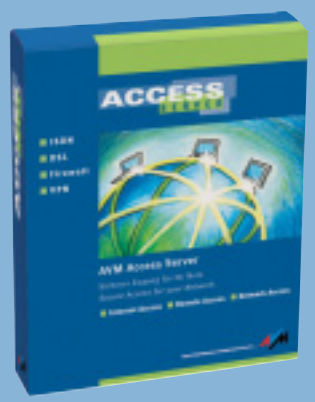
Bitte beachten Sie, dass NetWAYS/ISDN noch weitere wesentliche Leistungsmerkmale besitzt, die sich allerdings nicht auf den VPN-Einsatz beziehen. Weitere Leistungsmerkmale entnehmen Sie daher bitte dem gesonderten Datenblatt zu NetWAYS/ISDN.

AVM Access Server

- Umfangreiches VPN-Gateway und VPN-Concentrator
- Internetanbindung über ISDN-Wähl- und Festverbindung, DSL, GSM, HSCSD, Ethernet
- IPSec Transport- und Tunnelmode
- Authentication Header (AH, RFC 2402)
- Encapsulated Security Payload (ESP, RFC 2406)
- SHA-1, MD5
- DES, 3DES, AES
- IPComp RFC 2393 mit Deflate (RFC 2394), LZS (RFC 3051), LZJH (RFC 2395)
- Internet Key Exchange (IKE, RFC 2490), Main und Aggressive Mode
- Stateful Packet Inspection Firewall (Paket- und Portfilter, Input, Output, Forwarding)
- Skalierbarkeit über Basisanschluss- und Primärmultiplexkarten (BRI, PRI)
- Authentisierung über „preshared keys“ und X.509 Zertifikate
- Integrierte X.509-Zertifizierungsstelle

Systemvoraussetzungen

- Ab Intel Pentium 200 oder vergleichbarem Prozessor
- Windows 2003, Windows XP, Windows 2000 und Windows NT 4.0 (jeweils für Server und Workstation)
- 64 MB RAM
- 50 MB Festplattenplatz zur Installation, bis zu 250 MB Festplattenplatz im Betrieb (bei Protokollierung)



Bitte beachten Sie, dass der AVM Access Server noch weitere wesentliche Leistungsmerkmale besitzt, die sich allerdings nicht auf den VPN-Einsatz beziehen. Weitere Leistungsmerkmale entnehmen Sie daher bitte dem gesonderten Datenblatt zum AVM Access Server.

HIGH-PERFORMANCE COMMUNICATION BY ...

AVM Computersysteme Vertriebs GmbH · Alt-Moabit 95 · D-10559 Berlin · Tel. +49 (0) 30 / 3 99 76-0 · Fax +49 (0) 30 / 3 99 76-299 · www.avm.de · info@avm.de