

Testbericht Conware CoNet plus, SecuWare VPN-Manager und VPN-Client

# Überörtliche Verbindung

von Tim Kretschmann und Siegfried Streitz

Für die Verbindung zweier Standorte einer Kanzlei werden verschiedene technische Lösungen angeboten, die hinsichtlich ihrer Kosten genauer analysiert werden sollten. Die durch eine engere Zusammenarbeit entstehenden Vorteile dürfen nicht durch eine überproportionale Kostensteigerung zunichte gemacht werden, wenn z. B. auf einen gemeinsamen Adressbestand zur Kollisionsprüfung zugegriffen werden soll.

Eine mögliche Lösung ist der Aufbau eines internen Netzwerkes, das alle Standorte umfasst und auf der Betriebssystemebene realisiert wird. Damit wird grundsätzlich jede Software im Kanzleiverbund nutzbar, ohne dass sie besondere Standort-Eigenschaften besitzen muss. Allerdings muss geprüft werden, ob die Kapazität des Netzwerkes ausreichend ist und ob nicht zusätzlich bestimmte Funktionalitäten (z. B. Standort-gebundene Auswertungen) erforderlich sind.

Wie bereits in NJW-CoR 4/00 (S. 208ff) im Beitrag „Sicherheit und Datenkommunikation“ dargestellt, lassen sich verschiedene Systeme mit Hilfe von Stand- und Wählleitungen verbinden. Hierbei fallen jedoch erhebliche Kosten an, während bei der Benutzung des Internets und der verstärkt angebotenen Pauschaltarife (sog. Flatrate) eine für kleine und mittlere Unternehmen im Regelfall hinreichend leistungsfähige Verbindung zwischen zwei Standorten für weniger als 100,00 DM pro Monat aufgebaut werden kann.

Sie ist völlig ausreichend, um z. B. zwei Kanzleisysteme mit jeweils mehreren Dutzend Arbeitsplätzen zu verbinden, wenn die Software mit der Netzbandbreite sinnvoll umgeht. Hierzu wird ein virtuelles privates Netz (VPN – Virtual Private Network) aufgebaut, wie es in dem zitierten Beitrag beschrieben wurde.

Als Beispiellösung hat die Redaktion das Produkt CoNet plus Modell 2 mit der passenden Arbeitsplatz-Software

der Firma ConWare Netzpartner GmbH aus Karlsruhe getestet, das eine sichere Kommunikation über das Internet herstellt.

## Einführung

Zunächst wird kurz auf einige technische Sachverhalte zur Funktion des VPN-Routers und des VPN-Clients eingegangen. Weitergehende Informationen können dem genannten Beitrag in NJW-CoR 4/00 Sicherheit und Datenkommunikation entnommen werden.

Ein Router kann grundsätzlich die Verbindung eines lokalen Netzwerkes (LAN-Local Area Network) zu einem öffentlichen Netz (WAN-Wide Area Network) herstellen oder zwei LANs verbinden. Über diese Verbindung können dann Daten mit einem anderen Netzwerk oder Rechner ausgetauscht werden. Diese Verbindung ist ungeschützt und läuft meist im Klartext ab,

d. h. die Daten sind für jeden Rechner im Netzwerk lesbar und manipulierbar.

## Produktumfang

Das Produkt besteht aus zwei wesentlichen Komponenten: Das eigentliche Routergerät (CoNet plus), welches das LAN (Lokal Area Network = lokales Netzwerk) mit den vorhandenen Geräten (z. B. Drucker) externen Rechnern über eine VPN-Verbindung zur Verfügung stellt, und als zweite Komponente der SecuWare VPN-Client, ein Programm, das auf den externen Rechnern installiert sein muss, damit diese über das VPN Zugriff auf das LAN haben (s. Abb. 1).

### 1.1 CoNet plus

Neben dem von uns getesteten Modell 2 gibt es noch weitere CoNet-Modelle mit weiteren Ausstattungsstufen. Das getestete Modell umfasst die folgenden Komponenten:

- Gerät des Typs CoNet plus in der Größe eines kleineren Aktenordners
  - externes Netzteil zur Stromversorgung
  - 5 m langes ISDN-Kabel mit RJ45-Anschluss
  - Handbuch
  - sehr gute und ausführliche Online-Dokumentation
- Es stehen mehrere Anschlüsse zur Verfügung:
- ein oder mehrere ISDN-S0 Anschlüsse
  - verschiedene Netzwerkanschlüsse (10Base-T, 10Base5 und X21)
  - RS 232-Anschluss (V24) zur System-Konfiguration mit Hilfe eines Personalcomputers oder Terminals
- Folgende Funktionen, teils optional, unterstützt das Gerät:
- Brücken- und/oder Router-Funktionen (Funktionen zur Verbindung zweier Netzwerke)
  - verschiedene Protokolle (Protokolle

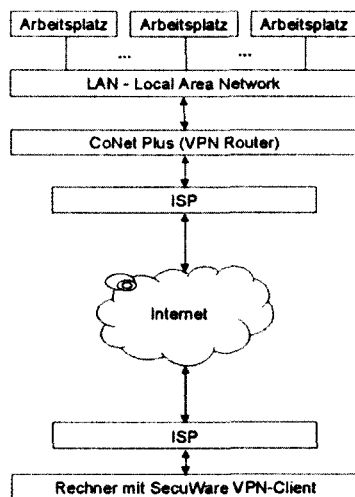


Abbildung 1: VPN (Virtual Private Network)

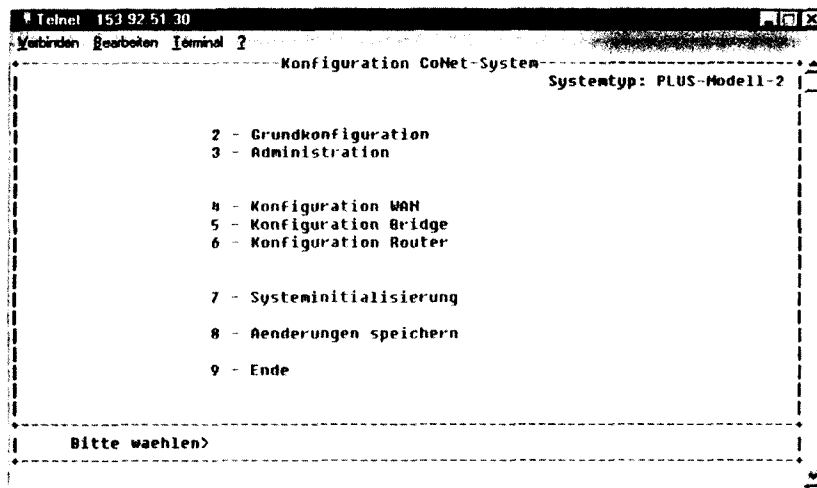


Abbildung 2: Administration des Routers über Telnet

sind Sprachvereinbarungen zwischen verschiedenen EDV-Systemen) für den Betrieb eines VPNs, die eine Verständigung möglich machen. Die wesentlichsten Protokolle sind IP, IPX, AppleTalk, IPSec. In einem VPN werden verschiedene solcher Protokolle unterstützt.

□ Router-Software zur Einrichtung und Wartung; die Router-Software ist update-fähig, d. h. sie kann später durch eine andere aktuelle Version ersetzt werden

Der Listenpreis für ein Gerät in Standardausstattung, das für die Verbindung zweier Standorte vollkommen ausreichend ist, beträgt 5.000,00 DM.

### 1.2 VPN-Client

Das Gerät CoNet plus wird im Hauptnetz eingesetzt, während die angeschlossenen Rechner (auch Einzelrechner) lediglich mit einem Modem oder einer ISDN-Karte und einer Software, dem sogenannten VPN-Client ausgestattet werden müssen, um auf das Hauptnetz Zugriff zu haben. Der VPN-Client mit dem VPN-Manager ist für die Betriebssysteme des Herstellers Microsoft Windows 95, 98 und NT 4.0 zu einem Listenpreis von 300,00 DM verfügbar.

Zum Test stand lediglich die Version 1.0 des IPSec Protokolls zur Verfügung, die aber nach Auskunft des Herstellers im Oktober 2000 durch die Realisierung

des neuen Standards IPSec Version 2.0 abgelöst werden soll.

### 1.3 Verschlüsselung

Über die Funktionalität eines VPN kann eine Verschlüsselung der Daten vorgenommen werden, so dass sie auf dem Weg über das öffentliche Telekommunikationsnetz nicht mehr lesbar sind. So wird eine sichere Datenverbindung geschaffen, die Datenintegrität, Vertraulichkeit und Verbindlichkeit gewährt. Bei einem solchen internen Netzwerk,

das öffentliche Leitungen nur als Übertragungsmedium benutzt, spricht man von einem VPN.

Die Verschlüsselung wird für den Benutzer transparent ausgeführt. Er braucht sich nicht um die Sicherheit beim Transport der Daten zu kümmern.

Zur Verschlüsselung kann ein Triple-DES-Verfahren mit einer Schlüssellänge von 112 Bit verwendet werden, das nach dem derzeitigen Stand der Technik als sehr sicher einzustufen ist. Als deutsche Produkte unterliegen die Conware-Systeme keinen Exportrestriktionen hinsichtlich des Verschlüsselungsverfahrens: es wird auch kein Masterschlüssel hinterlegt, wie es z. B. bei amerikanischen Produkten der Fall ist.

## Einsatz

Bei der Kontaktaufnahme eines externen Rechners über ein VPN mit dem LAN werden öffentliche Leitungen und insbesondere das Internet benutzt.

Beide Seiten der VPN-Verbindung, also der Router (hier CoNet plus) und der externe Rechner (s. Abb. 1) müssen dabei eine feste IP-Adresse haben. Eine IP-Adresse besteht aus einer Zahlenkombination, die vergleichbar ist mit einer Telefonnummer und jeden Teilnehmer eindeutig identifiziert. Diese festen IP-Adressen sind notwendig, da sie in einem Verzeichnis im Router und in der Client-Software VPN-Manager einge-

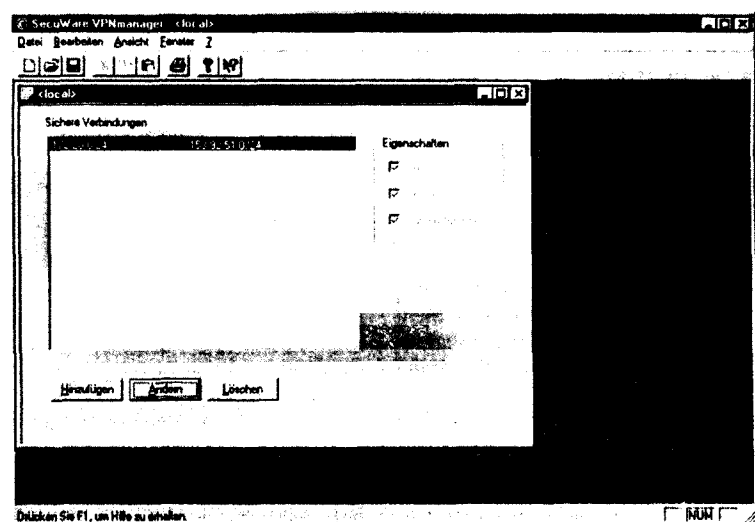


Abbildung 3: SecuWare VPN-Manager

tragen werden müssen, damit der Benutzer Zugang zum LAN erhält.

Mit der Version 1.0 ist es nur mit erheblichen Kosten möglich, von einem mobilen Anschluss aus mit Hilfe eines Internet-Zugangs am VPN teilzunehmen. Dieser Fall tritt z. B. beim Außer-Haus-Einsatz eines Notebooks auf. Wenn sich das Notebook ins Internet einwählt, so erhält es im Regelfall nur für die Zeit des Anschlusses eine bestimmte Adresse (sogenannte dynamische Adresszuweisung). Bei der nächsten Benutzung erhält das Notebook wieder eine andere Adresse. Da diese IP-Adressen nicht vorhersagbar sind, können sie somit auch nicht im Router und im VPN-Manager eingetragen werden. Die Verwendung von statischen Adressen ist demgegenüber sehr teuer.

Mit der neuen IPSec Version 1.2 ist eine Technik geschaffen, die das Einwählen eines Notebooks dennoch ermöglicht. Sie ist eine spezielle Version der Firma Conware, die jedoch kein Standard ist. Diese Version gibt es nur für den VPN-Client und den VPN-Gateway, aber nicht für den getesteten Router CoNet plus.

## Leistung CoNet plus

Der Router wird ins Netzwerk integriert. Er ist damit vom Betriebssystem unabhängig und arbeitet u. a. mit Microsoft Windows 95, 98, NT, Unix, Novell NetWare oder Novell IntranetWare zusammen.

### 1.4 Systemkonfiguration

CoNet ist mit Telnet über das Netzwerk oder über die V24-Schnittstelle administrierbar. Die Einrichtung des Systems (Konfiguration) kann bei CoNet über eine Menü-geführte Konfiguration (s. Abb. 2) oder über Kommandozeilen erfolgen. Die Menü-geführte Konfiguration ist teilweise durch Zuteilung mehrerer Namen (Aliasnamen) etwas undurchsichtig. Das für ein VPN zuständige Protokoll IPSec ist nur über Kommandozeilen zu konfigurieren.

Insgesamt ist die Konfiguration nicht endbenutzerfähig und nur für einen Techniker durchführbar.

### 1.5 Fehlerbehebung

Zur Kontrolle der Abläufe im VPN bietet die Firma Conware für ihr Produkt ausgezeichnete Möglichkeiten. So lassen sich Fehler im Netz sehr gut finden und aufklären. Als Beispiel ist denkbar, dass Daten verschickt werden, sie aber nicht an den Adressaten gelangen. Mit Hilfe des Routers CoNet plus ist es möglich zu erkennen, ob Daten verschickt wurden, ob diese verschlüsselt sind und an welcher Stelle im Netzwerk sie ggf. festsitzen.

Die Funktionen dazu sind jedoch ebenfalls nicht Endbenutzer-fähig. Allerdings dürfte es sich hierbei um Ausnahmefälle handeln, die hauptsächlich während der Erstinstallation auftreten.

Leistung VPN Client und Manager

Der VPN-Client hat die Aufgabe, die Einstellungen beim Aufbau einer VPN-Verbindung zu einer anderen Komponente (wie z. B. dem Router CoNet plus) umzusetzen.

Mit dem VPN-Manager werden die lokalen VPN-Einstellungen auf dem Client vorgenommen und verwaltet (s. Abb. 3).

## Sicherheitslücke

Da der Datentransfer über öffentliche Leitungen wie Telefon und Internet erfolgt, können sogenannte Hacker den Datenfluss mitschneiden und analysieren. Damit solche Personen die Daten nicht lesen können, sollten die Daten verschlüsselt verschickt werden.

Zur Verschlüsselung wird bei dem getesteten Gerät nach einer bestimmten Formel aus Sender- und Empfänger-Adresse ein Schlüssel berechnet. Diese Formel wiederum ist jedoch auch für einen erfahrenen Hacker entschlüsselbar. Um dies zu verhindern, sollten die Schlüssel per Hand auf einen anderen Wert gesetzt werden.

Das Modell CoNet und der VPN Manager der Firma Conware haben zwar die Möglichkeit, die Schlüssel manuell zu ändern. Dies kann jedoch nur von erfahrenen Technikern durchgeführt werden; die Bedienung ist nicht für einen Endbenutzer ausgelegt.

Andere Hersteller verhindern die Berechenbarkeit der Schlüssel, indem sie bei der Generierung vom Ersteller ein von ihm ausgewähltes Passwort verlangen. Die Möglichkeit zur Codierung der Schlüssel durch ein Passwort besteht bei CoNet nicht.

## Zusammenfassung

Das Produkt CoNet plus mit dem SecureWare VPN-Client bietet eine sichere Möglichkeit zur Einrichtung eines VPN. Die beschriebene Sicherheitslücke wurde auch vom Hersteller erkannt; die Beseitigung ist nach seiner Auskunft in Arbeit.

Die Produkte sind durch die Benutzung des IPSec-Standards mit anderen Systemen kompatibel. Das Preis-Leistungs-Verhältnis für CoNet plus ist durchaus zufriedenstellend, so dass dieses Produkt sowie der VPN-Client durchaus zu empfehlen sind. Darüber hinaus ist der Service der Firma Conware effizient strukturiert.

Ein Minuspunkt sind die Mängel im Rahmen der Benutzerfreundlichkeit des Routers. Die Einrichtung und Anpassung an Veränderungen ist für den Anwalt in der Regel nicht durchführbar, da er nicht über die nötigen Kenntnisse verfügt und er so seine Systeme nicht selbst verwalten kann.

Alternativ ist daher das Produkt Compact-Gateway in Betracht zu ziehen, das auch über den VPN-Manager zu verwalten und wesentlich benutzerfreundlicher als CoNet plus ist. Dieses Produkt besitzt jedoch keine Router-Funktion, so dass ein zusätzlicher Router bei Anbindung an ein WAN beschafft und eingerichtet werden muss.