

# ETS Fernzugriff auf eine KNX-Kundenanlage mittels VPN

Christian Ziegler  
Peter Sperlich

All-Com AG  
Siemens Schweiz AG

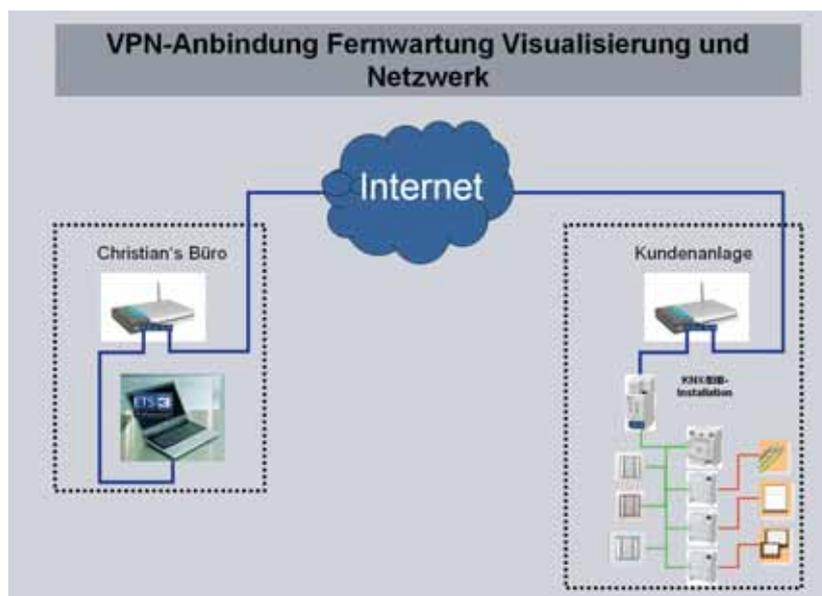


Bild 1. Prinzipschema einer Internetverbindung zweier Anlagen via VPN (Virtual Private Network)

**Die neuen KNX-Technologien ermöglichen zeitgemäße Lösungen. Auf eine der häufig angefragten Lösungen möchte ich in diesem Beitrag näher eingehen. Wie stelle ich eine VPN-Verbindung zum Kunden her, um eine Ferwartung durchzuführen? Und welche Geräte werden benötigt? Wie müssen diese konfiguriert werden? Was ist sonst noch zu beachten?**

In diesem Beispiel möchte ein KNX-Systemintegrator auf eine Kundenanlage via Internet zugreifen, um vom Kunden gewünschte Änderungen der Parametrierung von seinem Büro aus vorzunehmen. Der Systemintegrator nutzt hierzu die VPN-Technologie (VPN = Virtual Private Network). Hierfür benötigt der Integrator – nennen wir ihn „Christian“ – natürlich einen Laptop. Da er ein erfahrener und professioneller KNX-Systemin-

tegrator, verwendet er natürlich die aktuelle Inbetriebnahmesoftware der KNX Association; nämlich die ETS3professional. Christian besitzt in seinem Büro ein eigenes Netzwerk für die Kommunikation. Ein VPN-fähigen WLAN-Router ermöglicht über seinen Dienstanbieter die Verbindung zum Internet. (Siehe Bild 2). Als WLAN-Router bewährten sich



Bild 2. Laptop und VPN-fähiger Netzwerkrouter

Christian Ziegler ist Geschäftsführer der All-Com AG, Hofmannstr. 26, 8405 Winterthur, c.ziegler@all-com.ch

Peter Sperlich, Produktmanagement KNX Siemens Schweiz AG, Freilagerstraße 28, 8047 Zürich, peter.sperlich@siemens.com

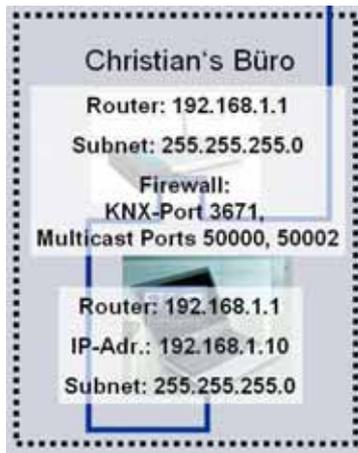


Bild 3. Adressvergabe im Büro von Christian



Bild 4. Die KNX-Kundenanlage mit KNX/IP-Router und VPN-Router

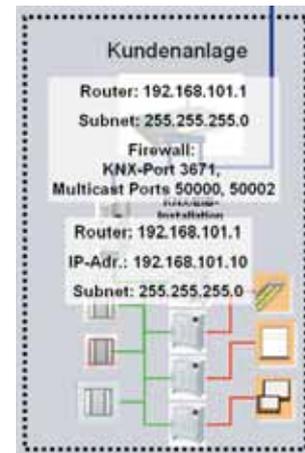


Bild 5. IP-Adressen in der Kundenanlage

bisher die Geräte der Firma ZYXEL (z. B. P-661H-D3).

Grundsätzlich spielt es keine Rolle, ob die IP-Adressvergabe beim Kunden fest eingestellt ist oder dynamisch läuft (DHCP). In diesem Beispiel benutzt Christian die Methode „feste IP-Vergabe“, innerhalb seines Netzwerks. (Siehe Bild 2) Im Netzwerk-Router „Zyxel“ sind in der Firewall die Ports für die Kommunikation über Multicast (50000 und 500002)

und der KNX-Kommunikations-Port (3671) freizugeben (siehe Bild 3).

In der Kundenanlage – im KNX-Haus – ist zur Anbindung ein KNX/IP-Router N146 integriert. (Siehe Bild 4) Das gleiche funktioniert aber auch mit der KNX/IP-Schnittstelle N148/21 oder mit dem KNX/IP-Controller N350E. Für die Verbindung zum Internet ist auch in der Kundenanlage ein VPN-fähiger WLAN-Router installiert. In der Kundenanlage sind

festen IP-Adressen für die Netzwerkkomponenten vergeben. (siehe Bild 5) und die Kommunikations-Ports, sowie der KNX-Port freizuschalten.

Nun geht es an die Konfiguration des VPN-Zugriffs des Netzwerkroters im Büro von Christian. In den VPN-Einstellungen des Netzwerkroters findet man die anschließend genannten Parameter (siehe Bild 6). Bei einer VPN-Verbindung wird „IPsec“ genutzt. IPsec (Kurzform für Internet

Bild 6. VPN-Einstellungen im Netzwerkrouter ZYXEL

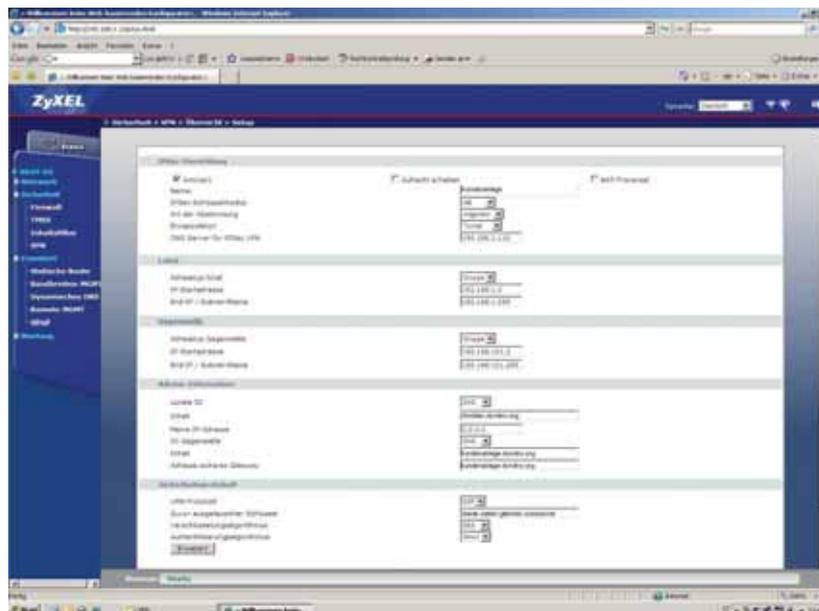
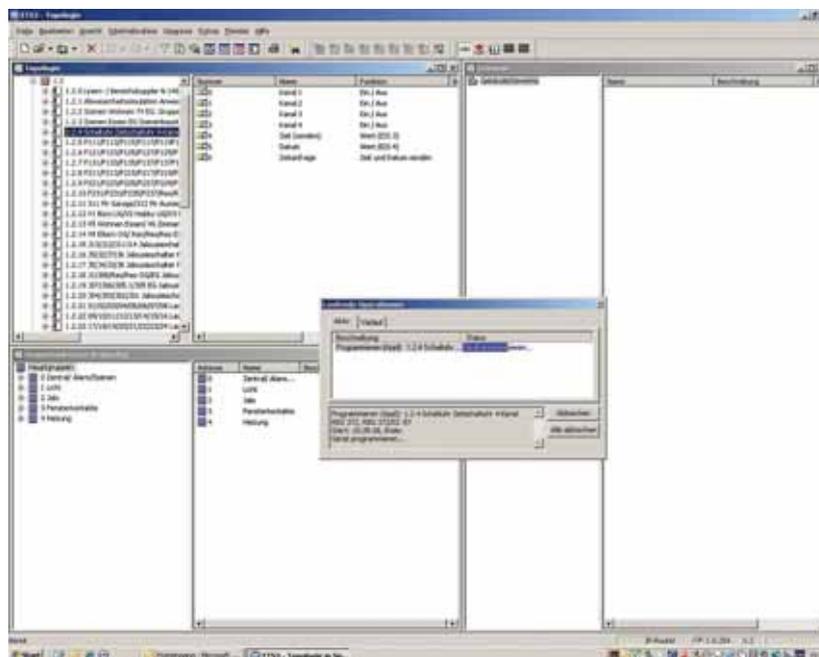


Bild 7. Laden der Parameter eines KNX-Gerätes mit der ETS3pro via VPN (Virtual Private Network)



Protocol Security) wurde 1998 entwickelt, um die Schwächen des Internetprotokolls (IP) zu beheben. Es stellt eine Sicherheitsarchitektur für die Kommunikation über IP-Rechnernetze zur Verfügung. IPsec soll die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten. In der IPsec-Konfiguration vergibt man zuerst einen Namen für die Verbindung. Da es sich um einen sicheren Tunnel handelt, ist die Art der Verschlüsselung anzugeben (hier IKE = Internet Key Exchange). Ausserdem die Art der Abstimmung (hier „Allgemein“), die Art der Verbindung („Tunnel“) und zuletzt die DNS-Server-IP-Adresse für die die VPN-Verbindung. Diese lautet bei VPN-Verbindungen immer 195.186.1.110. Anschliessend ist der Adresstyp (Adresstyp = Gruppe) und der IP-Adressbereich (IP-Startadresse = 192.168.1.0 und End-IP = 192.168.1.255) des lokalen Netzwerks zu benennen. Ebenso ist bei der Gegenstelle zu verfahren. Hier ist der Adresstyp ebenso eine „Gruppe“ und der IP-Bereich der Kundenanlage reicht von 192.168.101.0 bis 192.168.101.255.

Bei der Rubrik „Adress-Information“ sind nun die Internetadressen der beiden VPN-Partner anzugeben. In diesem Beispiel erstellte Christian sowohl für sich, wie auch für die Kundenanlage eine dynamische Webadresse beim Onlinedienst DynDNS (www.dyndns.org). Dieser Dienst leitet die sich wechselnde IP-Adresse des Internet-Routers des Internetanbieters auf eine fixe Webadresse um. In diesem Beispiel ist sinnigerweise die Domain von Christian „christian.dyndns.org“ und die des Kunden lautet „kundenanlage.dyndns.org“. Nun ist noch das Sicherheitsprotokoll für den VPN-Zugang zu definie-

ren (ESP = Encapsulation Security Payload) und ein entsprechender Schlüssel anzugeben. In der Kundenanlage geht Christian bei der Konfiguration des Netzwerkroters genauso, wie oben beschrieben vor. Einzige Ausnahme hierbei sind das gegensätzliche Austauschen der Parameter für „lokal“ und „Gegenstelle“. Die Konfiguration der Anlage sollte vor dem ersten Zugriff über das Internet in der Kundenanlage vom Integrator getestet werden. Das erspart unnötige Fahrerei zwischen Büro und Kunden. Ist der erste Zugriff erfolgreich, so steht der Inbetriebnahme per Internet zur Fernwartung nichts mehr im Wege.