NCP
SECURE COMMUNICATIONS

Funktionsbeschreibung und Konfiguration

high security remote access

L2Sec-Verschlüsselung für Enterprise Clients

L2Sec-Verschlüsselung für Enterprise Clients

In diesem Dokument ist die L2Sec-Verschlüsselung beschrieben, die nur vom Enterprise Client unterstützt wird.

Konfigurationseinstellung

Unter den Profil-Einstellungen des Enterprise Clients sind im Konfigurationsfeld **Security** die Parameter zu L2Sec und IPSec für den Einsatz in Remote Access-Umgebungen gesammelt.

L2Sec kann dann eingestellt werden, wenn als **VPN-Protokoll L2TP** für Layer-2-Tunneling gewählt wird. Dies erfolgt im Konfigurationsfeld Tunnel-Parameter.

L2Sec ist ein früher NCP-Standard und ein Alternative zur IPSec-Verschlüsselung. Alle Sicherheits-Verhandlungen erfolgen verschlüsselt und sicher in einem End to End-Tunnel (Layer 2) zwischen Client und Secure Server.

L2Sec nach RFC 2716

Die Praxis zeigt, dass es in VPN-Projekten gilt, einerseits eine sehr große Anzahl von verteilten PC-Arbeitsplätzen an die Firmenzentrale anzubinden und andererseits neben IP- auch IPX-, SNA- und NetBios-Datenpakete (native) zu übertragen sind.

Wichtig für die Sicherheit einzurichtender Kommunikationsnetze ist in besonderem Maße eine angemessene Authentisierung der Kommunikationsteilnehmer – bereits während des Verbindungsaufbaus. Dies ist umso vorrangiger, je mehr sich Mitarbeiter vom Telearbeitsplatz oder vom mobilen Büro über das Internet oder andere öffentliche Netze in das Datennetz des Unternehmens einwählen.

NCP hat L2Sec implementiert, um den Anforderungen der Unternehmen hinsichtlich offener Standards nachzukommen. L2Sec gilt sowohl vom Standpunkt der Sicherheit als auch der Kommunikation als Alternative zu IPSec. L2Sec vereint die Vorteile von L2TP mit Authentisierung und Verschlüsselung nach SSL (TLS). Dieses Verfahren ist im RFC 2716 (Microsoft) niedergelegt. NCP war nicht nur der erste Hersteller, der L2Sec implementiert hatte, lange bevor der RFC veröffentlicht wurde, sondern hat heute bereits auf die Bedürfnisse zahlreicher Großunternehmen, Organisationen und Behörden, die über die Unzulänglichkeiten von IPSec desillusioniert waren, erfolgreich reagiert.

L2Sec – Funktionsbeschreibung

Die PPP-Sicherheits-Verhandlungen erfolgen bei L2Sec, einer Layer 2-Verbindungen mit Security, sobald ein Kanal zum Zentralsystem aufgebaut ist. Layer 2-Kanäle können sein: ISDN B-Kanal, Modem-Verbindung, Tunnel (L2TP). Bei der NCP VPN-Tunneling-Lösung erfolgen alle Verhandlungsschritte verschlüsselt und sicher in einem End to End-Tunnel zwischen Client und VPN Gateway.

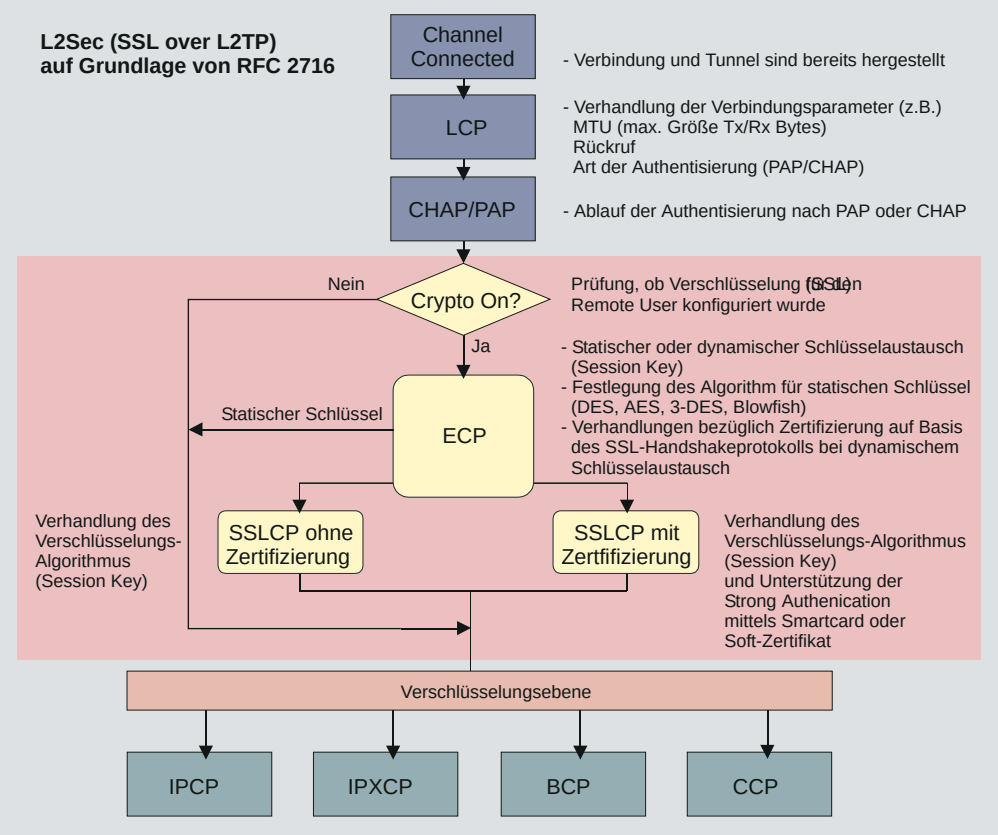
Dabei gewährleistet die Datenkommunikation über den End to End-Tunnel im virtuellen privaten Netz völlige Unabhängigkeit von der Kommunikationsumgebung. Der hierbei aufgebaute Tunnel, Geheimgang der Teilnehmer durch ein öffentliches Wählleitungsnetz, verläuft zwischen entferntem VPN Client und zentralem VPN Gateway.

Das komplette IP-Datenpaket, bestehend aus Nutzdaten und IP-Header, wird für die Übertragung verschlüsselt und mit einem neuen Header versehen. Mit anderem Worten: Auch die ursprünglichen IP-Quell- und Zieladressen unterliegen der Kryptierung – ein enormes Sicherheitsplus.

Zwischen dem VPN-Client und dem VPN-Gateway können auf der Wegstrecke des NCP End-to-End-Tunnels beliebig viele IP-Router unterschiedlicher Hersteller installiert sein. Diese müssen weder über Funktionalitäten zur Datenkompression und -Verschlüsselung noch über Tunneling-Protokolle verfügen.

Dies bedeutet Investitionsschutz und Offenheit pur, denn: In das Virtuelle Private Netz können somit sowohl Network Access Server von Internet Service Providern als auch bereits vorhandene eigene bzw. bei Geschäftspartnern installierte IP-Router integriert werden.

Auf diese Weise bildet die NCP Secure Software eine universelle Sicherheits-Infrastruktur, in die sich beliebige Business-Applikationen auf einfache Weise integrieren lassen. Ein zuverlässiges Schlüsselmanagement ist ebenso sichergestellt wie die Einbindung von Certificate Authorities (CAs).



LCP = Link Control Protocol
IPCP = Internet Protocol Control Protocol
CHAP = Challenge Authentication Protocol
IPXCP = Internetwork Packet Exchange Control Protocol
PAP = Password Authentication Protocol
ECP = Encryption Control Protocol
BCP = Bridge Control Protocol
SSLCP = Secure Socket Layer Control Protocol
CCP = Compression Control Protocol
L2Sec = Layer 2 Security ist funktionell im RFC 2716 beschrieben

Copyright

Network
Communications
Products engineering GmbH

Dombühler Str.2
D-90449 Nürnberg
Tel.: 0911 / 99 68-0
Fax: 0911 / 99 68-299
internet http:// www.ncp-e.com
E-mail: info@ncp-e.com