



DSL-Leitungen für ec-cash nutzen

Grundlagen

Trotz sinkender Kommunikationskosten nimmt die Position „DFÜ-Gebühren“ bei ec-cash Anwendungen immer noch einen nicht unerheblichen Stellenwert ein. Oft arbeiten die Kunden noch über einen ISDN-Anschluss der Telekom ohne sekundengenaue Abrechnung und bezahlen je online-Transaktion 7,75 Cent netto.

LAVEGO bietet mit dem Service SaveComm® eine sehr flexible und preiswerte Möglichkeit, die Kommunikationskosten erheblich zu senken (siehe Datenblatt „SaveComm® - immer preiswert kommunizieren“).

Wenn beim Kunden bereits eine DSL-Leitung vorhanden ist, kann de facto kostenlos über diese Leitung mit LAVEGO kommuniziert werden, da die kleinen Zahlungs-Datensätze praktisch kein Volumen verbrauchen. Aufgrund der mittlerweile guten Verfügbarkeit von DSL, der hohen Geschwindigkeit und der stark gesunkenen Preise bietet sich DSL als hervorragendes Übertragungsmedium für Zahlungsnachrichten an.

Die DSL-Leitung kann natürlich auch für andere Dienste genutzt werden. Speziell am PoS sind dies Kassenvernetzungen mit der Zentrale oder die Standarddienste email und Internet-Nutzung.

Sicherheit

Die Zahlungsnachrichten im ISO-8583 Protokoll sind zwar gegen Manipulation durch eine MAC (Message Authentication Code) geschützt – sie werden aber im Klartext (!) übertragen.

Es ist ein Leichtes, Bankverbindungen oder Kreditkartendaten beim ungeschützten Transport durch das Internet auszulesen und für betrügerische Zwecke zu mißbrauchen. Anders verhält es sich beim Transport z.B. durch das geschlossene Netz der Telekom bei ISDN; hier kann man nur mit hohem Aufwand Nachrichten abhören.

Aus diesem Grund muß der Datenverkehr durch das Internet vom PoS-Terminal zum Netzbetreiber verschlüsselt erfolgen.

Da es bei älteren Terminals aufgrund der geringen Rechenleistung des Prozessors nicht möglich ist, die Nachricht selbst bereits im Terminal zu verschlüsseln, muß dies nach dem Verlassen der Nachricht des Terminals geschehen.



Hier bietet sich ein VPN¹-Tunnel bis zum Netzbetreiber an. Es ist mit technisch vertretbarem Aufwand nicht möglich, die Nachrichten innerhalb des Tunnels zu entschlüsseln.

Auf der anderen Seite muß LAVEGO sicherstellen, daß die Anbindung des Rechenzentrums an das Internet ausfallsicher und v.a. sicher vor Angriffen aus dem Internet ist.

Deshalb wurde der Zugang zum Internet über 2 physikalisch verschiedene backbones realisiert. Jede Hardware-Komponente ist redundant vorhanden.

LAVEGO akzeptiert deshalb ausschließlich Daten, die über einen einwandfrei authentifizierten VPN-Tunnel geschickt werden. Zusätzlich werden die eingehenden Daten in Echtzeit daraufhin geprüft, ob es sich von Aufbau her um ISO-8583 Nachrichten gemäß der Schittstellenspezifikation von LAVEGO handelt.

Es ist nach jetzigem Wissensstand nicht möglich, ausführbaren Code innerhalb einer ISO-8583 Zahlungsnachricht zu übertragen.

LAVEGO betreibt ein redundant ausgelegtes VPN-Gateway, das als Endpunkt der VPN-Tunnel fungiert. Zu diesem Zweck werden für jeden Tunnel Zertifikate im X.509 Format erzeugt und bei der Konfiguration in die VPN-Router auf der Terminalseite eingebracht.

Das VPN ist technisch ein langes Netzkabel, das die Terminals direkt mit LAVEGO verbindet. Die Terminals erhalten deshalb auch gem. RFC1918 nicht durch das Internet leitbare private IP-Adressen, die von LAVEGO vergeben und verwaltet werden.

Einsatzszenarien

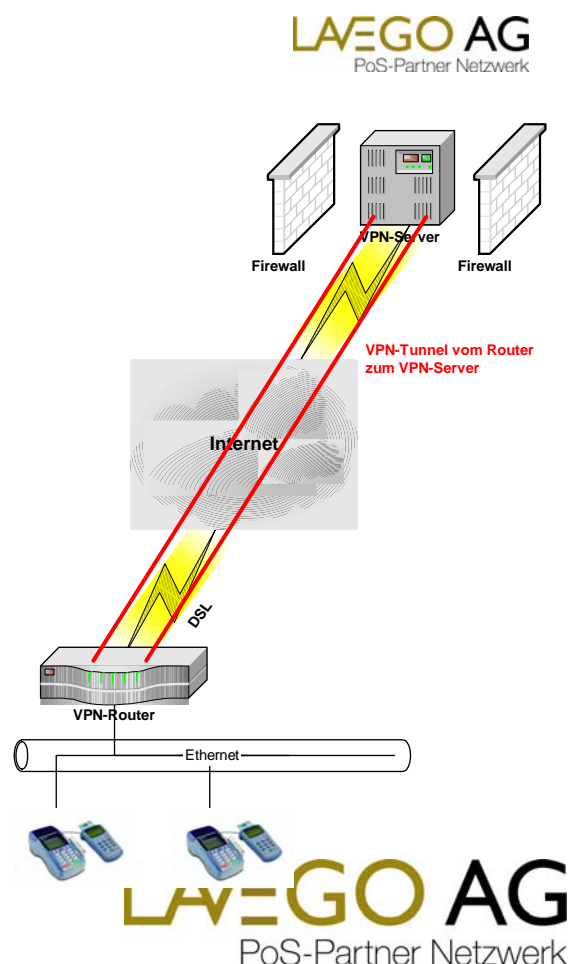
Ein oder mehrere Terminals an einer DSL-Leitung ohne ISDN-fallback

Diese Anwendung ist typisch für Installationen von einem oder mehreren Terminals mit hoher Transaktionszahl an einem Standort mit einer DSL-Leitung

Die Leitung wird ausschließlich für die Terminals genutzt; es sind keine weiteren Endgeräte angeschlossen.

Der Router baut selbständig den Tunnel zu LAVEGO auf und erneuert diesen, wenn er eine neue dynamische IP-Adresse vom DSL-Anbieter erhalten hat. LAVEGO setzt Router ein, bei denen dieser ca. 1-3 Minuten dauernde Stillstand automatisch in einer betriebsarmen Zeit (z.B. nachts) vom Router selbst ausgelöst wird.

Der Router verfügt neben dem DSL-Anschluss über keinen zusätzlichen ISDN-Anschluß, der die Kommunikation übernehmen kann, wenn DSL nicht verfügbar sein sollte.



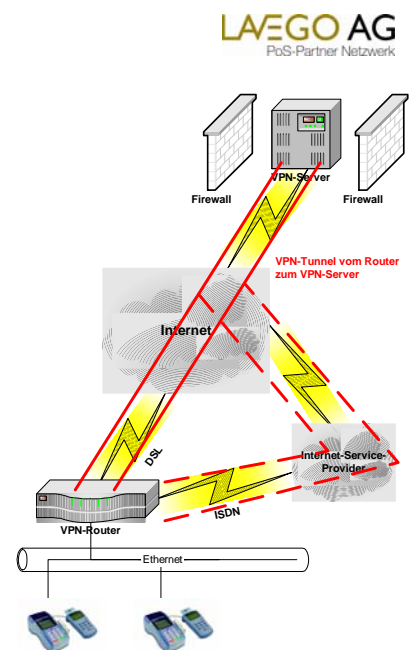
¹ VPN, virtual private network

Ein oder mehrere Terminals an einer DSL-Leitung mit ISDN-fallback

In diesem Fall wird ein aufwändigerer (=etwas teurerer) Router verwendet, der parallel zum DSL-Anschluß auch über einen ISDN-Port verfügt. Ansonsten ist die Installation identisch wie oben.

Der Router stellt selbständig eine ISDN-Wählverbindung zu einem beliebigen ISP (Internet-Service-Provider) her und baut den VPN-Tunnel auf, wenn die DSL-Verbindung nicht funktionieren sollte.

Im Hintergrund wird geprüft, ob DSL wieder funktioniert und entsprechend zurückgeschaltet.



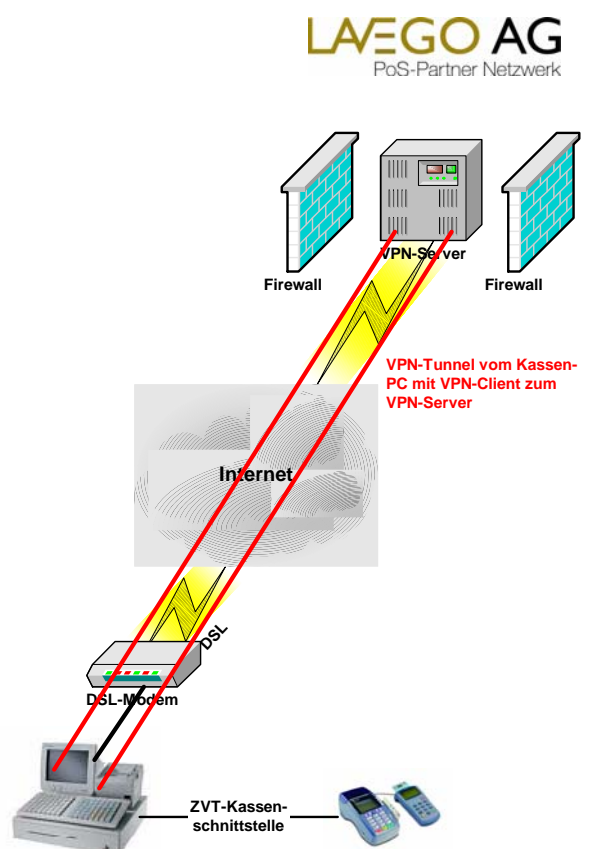
Terminals mit Kassenanbindung und Software-VPN-Client

Im Folgenden wird mit „Kasse“ immer eine Einheit bezeichnet, die das Terminal über die ZVT-Kassenschnittstelle ansteuert. Das kann auch ein Waren- oder Tankautomat sein. Das Terminal kann auch die in der Kasse evtl. vorhandene DFÜ-Einheit mitbenutzen; die Schnittstelle gestattet dies explizit.

Anstelle eines (Hardware)Routers kann ein VPN-Tunnel auch von der Kasse mit Hilfe eines VPN-Software-Clients aufgebaut werden.

Der Softwareclient ist preiswerter als ein Router; er bietet sich deshalb an, wenn nur eine Kasse mit einem Terminal an DSL angeschlossen werden muss.

Wenn mehrere Kassen an einem Standort zum Einsatz kommen, müsste jede Kasse einen eigenen Software-Client haben, was bereits bei 2-3 Kassen meist teurer als ein Router ist.



Terminal und Kasse mit jeweils eigener VPN-Vernetzung; keine andere Nutzung

Alle von LAVEGO eingesetzten Router können mehrere VPN-Tunnel gleichzeitig verwalten.

Speziell für den Austausch von Warenwirtschaftsinformationen mit der Zentrale bei modernen Kassensystemen bietet sich eine schnellere Verbindung als ISDN an.

LAVEGO nutzt beim VPN v.a. den extrem schnellen Austausch der kleinen Datensätze von Zahlungen; die Kassensysteme profitieren v.a. von der deutlich schnelleren Datenübertragung bei DSL.

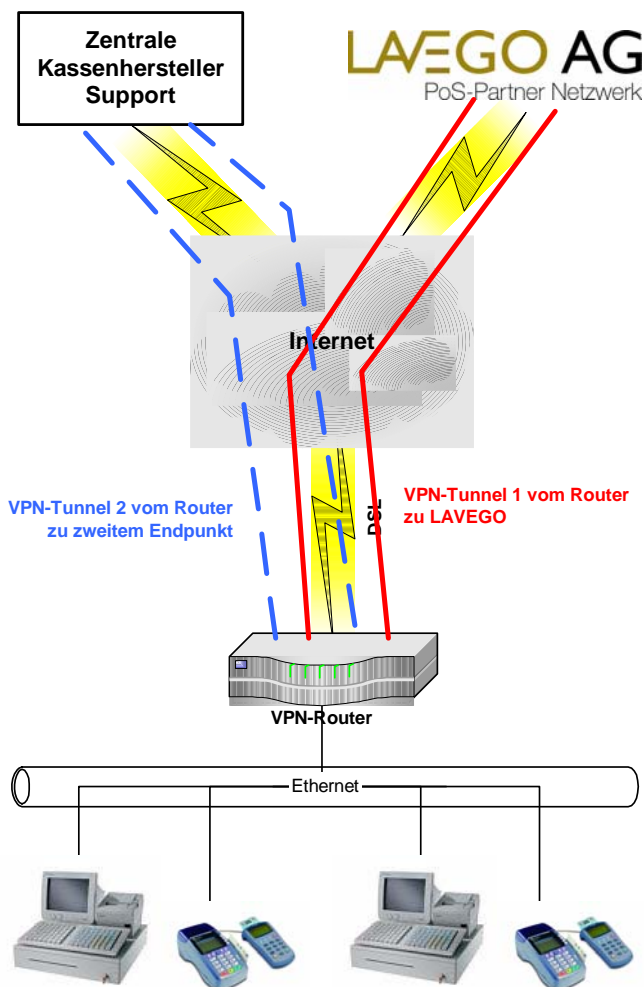
In der Zentrale muss entsprechende Hardware zur Verfügung stehen, um den zweiten VPN-Tunnel zu terminieren.

Während in den Filialen sicherlich A-DSL Leistungen ausreichen („A“ steht für asynchron; dabei ist die Up- und Downloadgeschwindigkeit unterschiedlich. Normalerweise kann mit 1-6 MBit / s aus dem Internet heruntergeladen werden, aber nur mit 128-192 KBit / s Datenverschickt werden), sollte in der Zentrale eine S-DSL Leitung verwendet werden. „S“ steht für synchron und bedeutet gleiche Up- und Downstream-Geschwindigkeiten bei der Leitung. S-DSL-Leitungen sind üblicherweise teurer als A-DSL-Leitungen.

In diesem Beispiel wird davon ausgegangen, dass die A-DSL-Leitung ausschließlich für die Kassen und PoS-Terminals genutzt wird und keine weitere Nutzung für emails oder Internetsurfen erfolgt. Genau dann ist die Anbindung per Router und ausschließlicher VPN-Nutzung relativ sicher.

Sollte jemand „heimlich“ jedoch einen PC mit email-Verkehr an den Router anschließen, könnte es passieren, dass Viren über den sicheren Tunnel zur Zentrale gelangen und dort Schaden anrichten.

Der Tunnel bietet ja nur die Sicherheit, dass beim Weg durch das Internet niemand die Daten mitlesen kann. Wenn Viren bereits vor dem Tunnel vorhanden sind und durch den Tunnel hindurch geleitet werden, bieten auch firewall-Systeme keinen ausreichenden Schutz, weil diese auch nicht in den Tunnel hinein schauen und dort schädlichen Code entdecken können.



Terminal und Kasse mit jeweils eigener VPN-Vernetzung; zusätzliche Nutzung z.B. für email und Internet

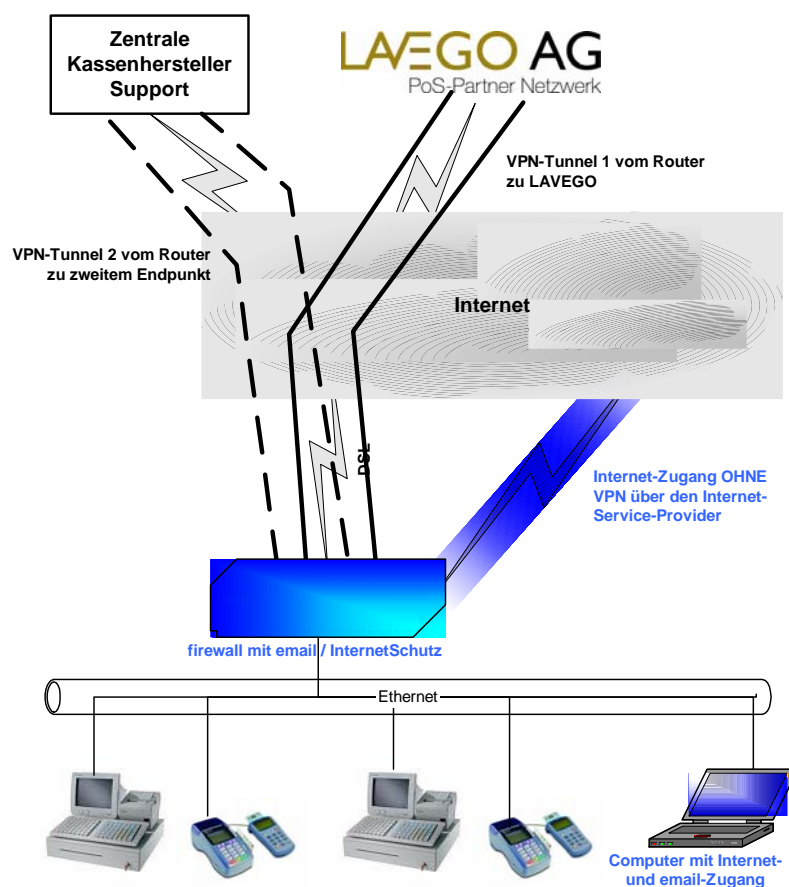
Um die Gefahr zu vermeiden, dass schädlicher Code in die VPN-Tunnel gelangen kann (siehe Beispiel oben) und trotzdem andere Rechner das Internet nutzen können, müssen Schutzmaßnahmen ergriffen werden.

Die meisten der von LAVEGO verwendeten Router besitzen eine integrierte Firewall mit „stateful inspection“. Diese betrachtet neben den normalen Paketfilter-Optionen zusätzlich den Status der Verbindung in das Internet und hinterlegt alle aktuellen Verbindungen in einer dynamischen Tabelle. Dabei werden die aktuellen Zustände von Verbindungsaufbau, Transfer / aktive Verbindung und Verbindungsabbau festgehalten.

Im Ergebnis werden prinzipiell nur Pakete in das interne Netz gelassen, für die bereits aus diesem Netz initiierte Verbindungen bestehen. Pakete von außen, die nicht einer dieser Verbindungen zuzuordnen sind, werden verworfen und im Log-File protokolliert.

Eine noch größere Sicherheit erhält man, wenn zusätzlich Services genutzt werden, die eingehende emails oder den Datenstrom vom Internetsurfen auf schädlichen Code (Viren, Trojaner usw.) untersuchen und v.a. regelmäßig automatisch aktualisiert werden.

LAVEGO bietet als Dienstleistung die Planung, Einrichtung und den Betrieb eines VPN-Netzwerkes an. Dazu gehört auch die Beantragung der Leitungen und die Überwachung der Installation. Wir greifen dabei auf Komponenten der deutschen Hersteller Astaro (www.astaro.de) und bintec (www.funkwerk-ec.com) zurück.





IP-Telefonie (VoIP, Voice over IP)

Bei den meisten A-DSL-Leitungen der großen freien Anbieter ist es mittlerweile möglich, auch über das Internet zu telefonieren. Das Telefonieren von einem zum anderen VoIP-Nutzer ist meist kostenlos (auch weltweit); Gespräche in das deutsche Festnetz kosten nur 1-2 Cent / Minute.

Die aktuell angebotenen und im Preis der DSL-Leitung enthaltenen Router (z.B. AVM Fritz! Box DSL) haben 1-2 analoge Telefonbuchsen zum Anschluss von Endgeräten (z.B. DECT-Funktelefone).

Da die meisten DSL-Anschlüsse im Businessbereich auf ISDN-Anschlüsse aufsetzen, kann der VoIP-Router parallel auch an den ISDN-Basisanschluß (nicht Anlagenanschluß) angeschlossen werden.

Eingehende Anrufe gelangen über ISDN an den Router, der auf die analogen Endgeräte – wie eine kleine Telefonanlage – umwandelt.

Bei ausgehenden Anrufen kann in einer Routingtabelle definiert werden, ob VoIP oder ISDN genutzt werden soll.

Es ist jedoch zu bedenken, dass sich die Einrichtung und der Betrieb eines solchen Netzwerkes nur rechnet, wenn sehr viel telefoniert wird. Ist dies der Fall, sollte die DSL-Leitung über eine Flatrate verfügen, da der Datenstrom beim Telefonieren nicht unerhebliche Datenmengen produziert.

Problematisch ist auch die meist unverschlüsselte Übertragung bei VoIP; geschäftliche Telefonate sollten ausschließlich über ein VPN mit dem Partner geführt werden.

Überwachung, Monitoring

Ein wichtiger Aspekt – gerade bei der Nutzung von unbedienten Automaten – ist die permanente Überwachung der Funktionsfähigkeit. Während bei einem bedienten Terminal ein Ausfall sofort bemerkt wird, kann ein nicht funktionierender Automat tagelang unentdeckt bleiben.

LAVEGO überwacht alle VPN-Tunnel permanent und bekommt Warnhinweise, wenn der Tunnel nicht mehr zur Verfügung steht, sich die Bandbreite des Routers erheblich verschlechtert oder wenn das angeschlossene Terminal nicht mehr erreichbar ist. Auch wird das Umschalten auf ISDN signalisiert, so dass aktiv reagiert werden kann.