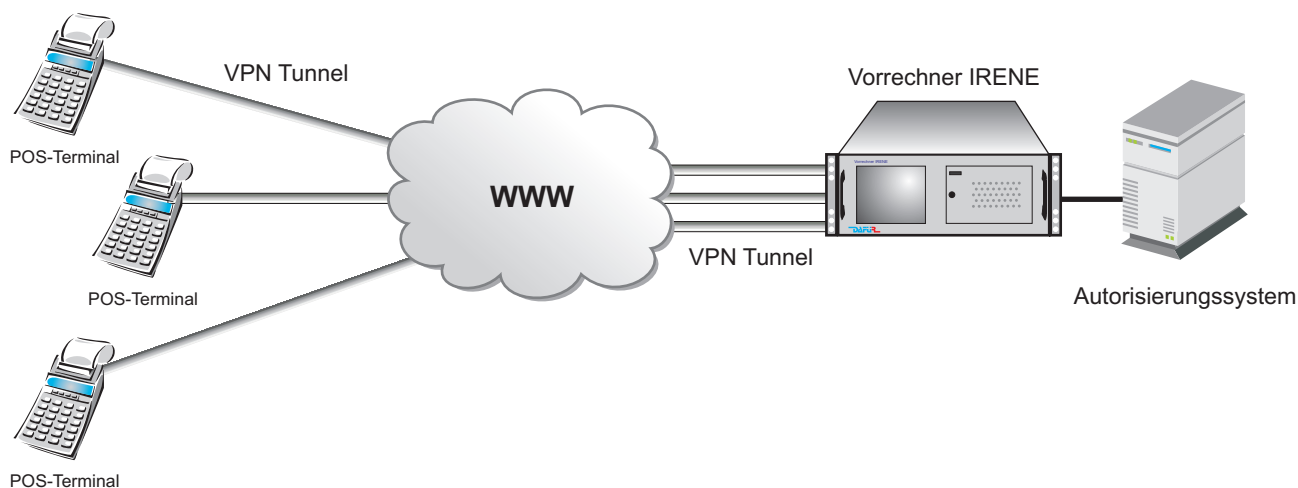


POS-Terminals mit VPN einfach und sicher mit

IRENE*



POS-Terminals mit Zugang übers Internet (VPN) finden immer mehr Verbreitung

Wenn POS-Terminals ihre Anfrage nach einer Kartenautorisierung übertragen, wird hierfür traditionell das ISDN-Netz verwendet. Dabei halten sich der Analogbetrieb über Modems und der Betrieb über X.31 im B-Kanal die Waage. Die Tendenz ist dabei klar, der Betrieb mit X.31 im B-Kanal wird zunehmen, der Analog-Modemverkehr wird abnehmen. Der Anteil von Terminals, die mit GSM den ISDN-Dienst V.110 verwenden, liegt, je nach Netzbetreiber, zwischen 5 und 10 %.

Der Trend, das Internet für Nachrichtenübertragung jeglicher Art zu verwenden, ist unübersehbar, keine Firma ist ohne Internetanschluß, über 80% aller privaten Haushalte sind am Internet angeschlossen. Auch die Übertragung von Sprache, traditionell eine Aufgabe des öffentlichen ISDN-Netzes, wird durch Voice over IP (VoIP) nach und nach ersetzt.

Von diesem Trend können sich POS-Terminals nicht abkapseln. Durch Verpackung der ISO-Transaktionen in TCP/IP scheint das Problem gelöst zu sein, zumal auch die Autorisierungssysteme direkt TCP/IP fahren. Dadurch

können auf den ersten Blick POS-Terminals und Autorisierungssysteme direkt miteinander verbunden werden.

Wer dies jedoch tut, wird große Überraschungen erleben!

Im Folgenden wollen wir die verborgenen Kosten einer solchen Anbindung aufdecken und zeigen, wie man diese minimieren kann.

Zugang nur über VPN

Das Hauptziel beim Entwurf des Internet in den 60er Jahren war, ein Netz und ein Datenprotokoll zu

schaffen, das sicherstellt, dass jeder Teilnehmer jederzeit erreichbar ist. Dieses Ziel wurde zu 100% erreicht, die Router im Internet finden immer Ausweichwege, sollte eine direkte Verbindung einmal gestört sein.

Gesicherte und authentifizierte Datenübertragung war jedoch kein Designziel, entsprechend muss der Anwender dafür Sorge tragen, will er sensitive Daten übertragen. Und beim Bezahlen mit Karten liegen mit Sicherheit sensitive Daten vor.

Durch die Etablierung eines virtuellen privaten Netzwerkes (VPN) wird ein durch Zertifikate

*Intelligente Rechnerinheit mit Netzwerkeinbindung

und/oder Schlüsselverfahren gesicherter Tunnel zwischen den Netzteilnehmern A und B, hier also zwischen dem POS-Terminal und dem Autorisierungssystem aufgebaut.

Der Aufbau einer Verbindung wird durch Passwörter geprüft und gesichert. Kein Unbefugter kann in eine bestehende VPN-Datenverbindung eindringen und damit Datenströme manipulieren.

Na also, könnte man sagen, über VPN lässt sich ein POS-Terminal sicher an ein Autorisierungssystem anschließen. Das ist so richtig. Sinnvoll ist sowas aber nur, wenn man nur **ein** POS-Terminal in Betrieb hat, und das ist eine unsinnige Voraussetzung.

NAT ohne Verlust der Absendeadresse

Bild 1 zeigt, wie die einzelnen Komponenten eines POS-Autorisierungssystems im Internet zusammen geschaltet sind.

Jede Verbindung im Internet braucht im IP-Protokoll eine eindeutige Quell- und Ziel-IP-Adresse und im TCP-Protokoll einen eindeutigen Quell- und Ziel-Port. Betrachten wir ganz kurz den Ablauf einer POS-Autorisierung im Internet:

Die Initiative geht vom POS-Terminal aus, dieses äußert über das Point-to-Point Protokoll (PPP) einen Verbindungswunsch.

Vom Internetbetreiber wird dem lokalen Gateway eine IP-Adresse aus dem Adresspool des Internet-

Der Vorrechner IRENE - Ihr zentraler Anschluss für POS-Terminals via VPN

- Zugang nur über VPN
- NAT ohne Verlust der Absendeadresse
- TCP-Portnummer im Call-User-Datafield
- Integrierter Loadbalancer auf Applikationsbasis
- Abbildung der ISDN-Nummer auf IP-Adresse und Port-Nummer
- Nur formatgeprüfte Informationen kommen zum Zielsystem
- höchstmögliche Sicherheit durch Application Layer Firewall
- Accounting Informationen
- einfache Terminalkonfiguration und Tests
- Routing aus ISO-Nachrichten heraus möglich
- timergesteuerte Verbindungsüberwachung
- sicher gegen TCP-Attacks

providers temporär zugewiesen, die für die Dauer der Verbindung ihre Gültigkeit hat. Mit dieser zugewiesenen IP-Adresse kommt die Anfrage beim Vorrechner IRENE an, dieser prüft, ob Quell- und Ziel-Port mit Tabelleneinträgen übereinstimmen und reicht die Anfrage mit der IP-Adresse an die Firewall weiter.

Das können herkömmliche Router auch. Allerdings geht bei diesem Verfahren die Quell-IP-Adresse des Terminals verloren, da der NAT-Dienst (Network Address Translation) als Quell-Adresse die Ziel-Adresse des Routers einsetzt.

Damit geht die IP-Adresse des Terminals verloren; bei Störungen im Internet, haben Sie keine Aussage mehr, welche Terminals an einem bestimmten Tag durchgekommen sind und welche nicht.

Der Vorrechner IRENE kann jedoch die IP-Adresse wie eine

rufende X.25-Adresse in den Datenstrom einfügen, Sie finden damit in einem X.25-Log stets eine Übersicht, welche Terminals anhand der IP-Adresse aktiv waren oder nicht.

Herkömmliche Router liefern Ihnen diese Informationen nicht.

Sie können damit im Störfall die Störungsursache viel schneller eingekreisen und Ihren Kunden eine intakten Dienst wieder zur Verfügung stellen.

TCP-Portnummer im Call-User-Datafield

Die Terminals müssen immer an einen bestimmten Port auf dem Applikationssystem geroutet werden. Eine übliche Methode ist, im Call-User-Datafield (CUD) die gewünschte TCP-Zielpportnummer einzutragen.

In herkömmlichen Routern muss

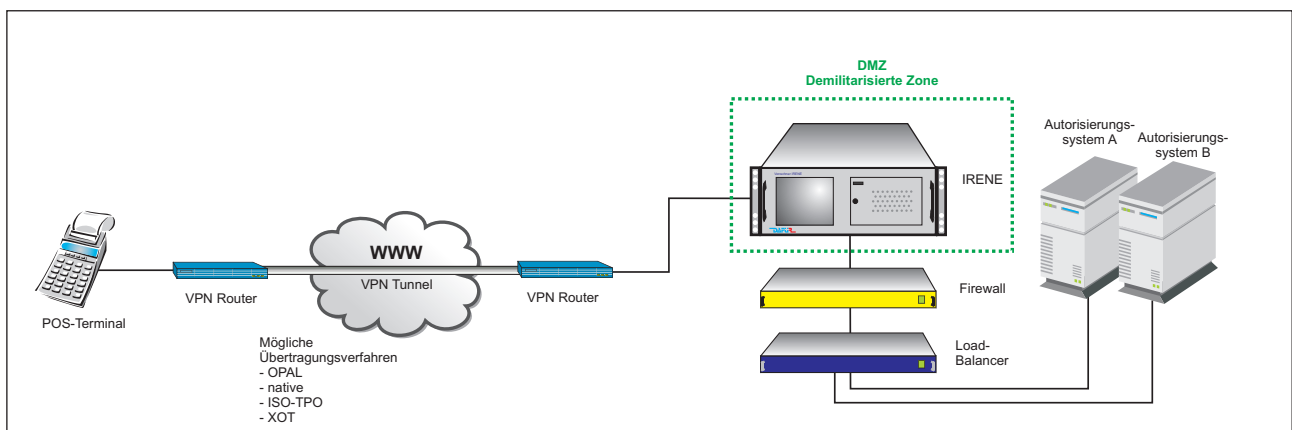


Bild 1: Prinzipielle Verknüpfung von Netzwerkkomponenten zum Aufbau eines POS-Autorisierungssystems über das Internet und VPN.

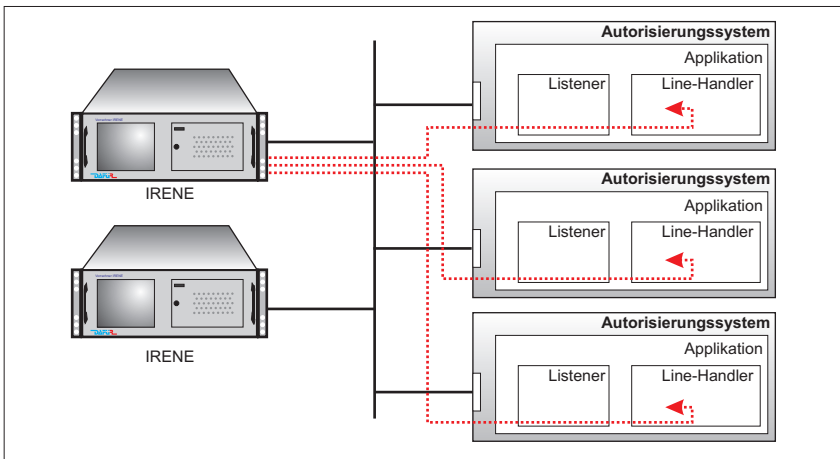


Bild 2: Überprüfung der Verfügbarkeit von Autorisierungssystemen auf Applikationsebene und Loadbalancing

also eine Tabelle gepflegt werden, die jedem CUD den entsprechenden TCP-Zielport zuordnet. Dies kann bei der Terminalvielfalt im Markt ziemlich aufwändig werden.

Der Vorrechner IRENE liest das CUD aus und setzt den gelesenen Inhalt für den TCP-Port-Verbindungsaufbau ein. Eine Pflege von Tabellen ist damit hinfällig!

Ihre Netzwerkadministratoren verschwenden keine Zeit mit der Pflege langweiliger Tabellen.

Integrierter Loadbalancer auf Applikationsbasis

Der Load-Balancer verteilt die ankommende Last auf mehrere Autorisierungssysteme, so dass diese

- gleichmäßig ausgelastet sind und
- im Störfall die Anfragen

nur noch an die intakten Autorisierungssysteme weitergeleitet werden.

Ob ein Autorisierungssystem verfügbar ist oder nicht, prüfen herkömmliche Loadbalancer durch einen "Ping". Ob allerdings der zugehörige Listener-Prozess und der Line-Handler auf Applikationsebene aktiv ist, können diese Systeme nicht feststellen.

Der Vorrechner IRENE geht hier viel weiter und stellt bis in die höchste Ebene sicher, dass Ihr Autorisierungssystem wirklich verfügbar ist. IRENE sendet dazu in zyklischen Abständen eine Diagnosenachricht, die von der Applikation beantwortet werden muss.

Wird diese Diagnoseantwort in der vorgegebenen Zeit von IRENE empfangen, gilt diese Weg als intakt, ist das nicht der Fall, wird ein SNMP-Alarm abgesetzt und Sie sind sofort informiert, sollten die Autorisierungssysteme einmal hängen.

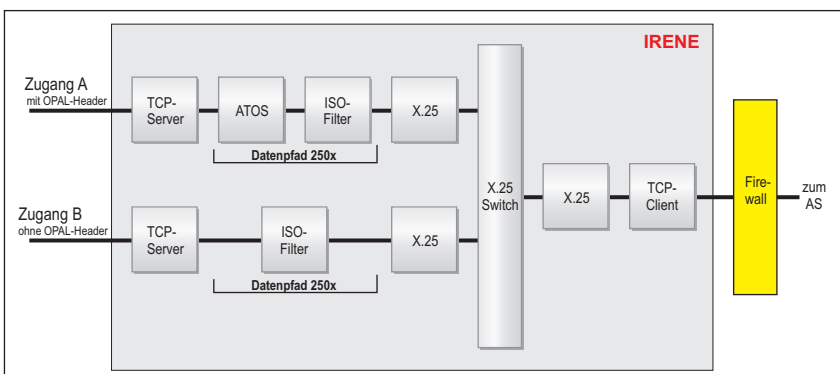


Bild 3: Zusammenschaltung der Softwarekomponenten im Vorrechner IRENE zum Betrieb von POS-Terminals über VPN

Der Vorrechner IRENE verteilt danach zyklisch die ankommende Last an die aktiven Systeme.

Dieses Loadbalancing liefert Ihnen kein auf dem Markt verfügbares System!

Abbildung der ISDN-Nummer auf IP-Adresse und Port-Nummer

Haben Sie neben den VPN-Zugängen auch Terminals in Betrieb, die sich über ISDN einwählen, so lassen sich auf dem Vorrechner IRENE ISDN-Durchwahlen definieren, denen Sie dann die gewünschte IP-Adressen oder Port-Nummern auf dem Autorisierungssystem zuweisen.

Das eröffnet Ihnen die Möglichkeit, auch analoge Terminals mit unterschiedlichen Betriebsarten, für die Sie jeweils eine Durchwahl vorsehen, auf die zugehörigen Systeme mit den gewünschten IP- und TCP-Adressen zu routen.

Ein Beispiel für ein solches Routing wäre:

ISDN-Zielnummer	soll geroutet werden auf IP-Adresse/TCP-Port
140010	192.1.2.50 Port 10000
140022	192.1.2.50 Port 10005
140033	192.1.2.49 Port 10006

Eine solch einfache Zuordnung werden Sie in herkömmlichen Routern nicht finden.

Nur formatgeprüfte Informationen kommen zum Zielsystem

Betrachten wir zunächst den oberen Pfad (siehe Bild 3), den Zugang A mit Opal-Header. Mit diesem Opal-Header wird sichergestellt, dass die Blockinformationen eines ISO 8583 Blockes erhalten bleibt. Zwei der ISO-Informationen vorangestellte Byte hex-codierter Länge stellen sicher, wann der ISO-Datenblock beginnt und wann er aufhört.

Ein großer Anteil der POS-Terminals sendet seine Anfragen

bereits in diesem Format. Im Softwaremodul „TCP-Server“ wird der ankommenden Anruf entgegengenommen und die Verbindung nach Überprüfen von TCP- Quell- und Zielport aufgebaut.

Die ankommenden Daten müssen dem von ATOS vorgegebenen Längenformat entsprechen und der „ISO-Filter“ prüft, ob es sich um komplette ISO-Nachrichten handelt. Dann und nur dann wird die Nachricht über „X.25“ und den „X.25-Switch“ an ein aktives Autorisierungssystem über den „TCP-Client“ weitergereicht.

Sollten die Terminals ihre Nachricht zwar im TCP-Format, aber ohne Opal-Header senden, (also native), so ist dies über einen anderen TCP-Zielport im Verbindungsaufbau mitzuteilen und die Anfragen werden im unteren Datenpfad verarbeitet.

Höchstmögliche Sicherheit durch Application Layer Firewall (ALF)

Das oben beschriebene Verfahren gibt Ihnen die größtmögliche Sicherheit, dass nur die gewünschten Informationen bei Ihren Autorisierungssystemen ankommen. Alle Attacken, Viren und ähnlicher Internetmüll wird vom ISO-Filter erfolgreich unterdrückt, da er nicht nur wie eine Firewall IP-Adressen und TCP-Ports prüft, sondern in die Applikation der ISO-Daten eingeht.

Keine Firewall auf dem Markt besitzt diese Mächtigkeit!

Diese Vorgehensweise stellt Ihnen ebenfalls sicher, dass die nachgeschaltete Firewall ausschließlich mit der Quell-IP-Adresse der IRENE eingestellt werden muss, die zufällig vergebenen IP-Adressen auf der Netzseite werden vom Vorrechner IRENE berücksichtigt.

Accounting Information wird erzeugt

Der Vorrechner IRENE stellt für jede ankommende Transaktion,

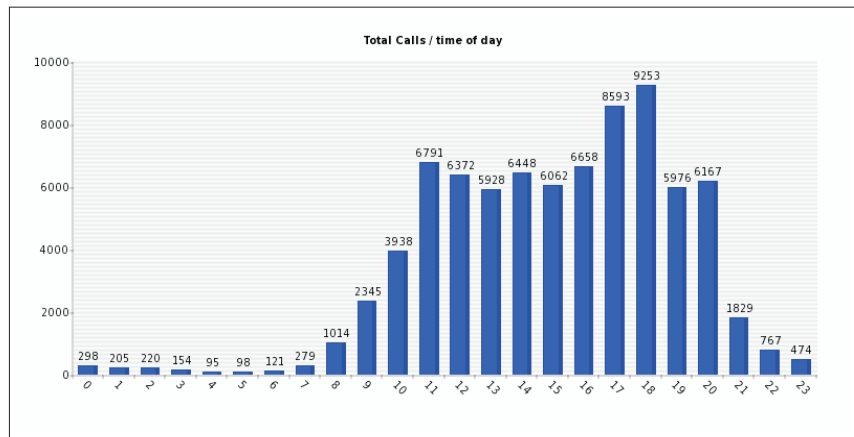


Bild 4: Darstellung der Auslastung einer IRENE durch Auswertung der Accounting Informationen

gleichgültig, ob sie über ISDN, X.25 oder VPN eingegangen ist, einen Logeintrag zusammen, der Datum, Uhrzeit, IP- und TCP-Adressen, ISO-Datentyp, Terminal-ID und Blocklänge enthält.

Diese Informationen können von einem Server in Ihrem Hause entgegengenommen und statistisch ausgewertet werden.

Sie können sich damit einen Überblick über Verteilung von Nachrichtentypen, Terminaltypen, zeitliche Auslastungen über den Tag, über die Woche und den Monat verschaffen.

Tests von neuen Terminals und Softwareständen

Der Vorrechner IRENE eröffnet Ihnen die Möglichkeit, dedizierte Testzugänge einzurichten, über die einzelne Terminals, sei es im Falle von Betriebsproblemen oder bei Abnahmen bzw. Integrationstests neuer Terminaltypen oder Softwarestände, eingangsseitig entgegengenommen, jedoch nicht an ein Produktivsystem weitergeleitet werden. Mithilfe der in IRENE integrierten mächtigen Tracemöglichkeiten kann dann innerhalb kürzester Zeit eine Aussage über das Betriebsverhalten des Terminals getroffen werden.

Um diese Testmöglichkeit zu nutzen, ist am zu prüfenden Terminal nur ein Parameter zu verändern, nämlich die Zielportnummer.

Das Autorisierungssystem hingegen bleibt unverändert.

Routingmöglichkeiten aus der ISO-Nachricht

IRENE unterstützt neben dem Routing anhand der vom Terminal angesprochenen TCP-Portnummer auch ein Routing aufgrund von Merkmalen der vom Terminal geschickten ISO 8583-Nachricht.

Zum Routing verwendet werden können ein oder mehrere der folgenden Felder der ISO 8583-Nachricht:

- Nachrichtentyp (0200, 0400, 0800, etc.)
- Processingcode
- Terminal-ID (einzelne Terminal-ID's bzw. Gruppen von Terminal-ID's)

Anhand einer im laufenden Betrieb änderbaren Routingtabelle können ISO 8583-Nachrichten zu verschiedenen Zielsystemen, die über TCP/IP oder X.25 erreichbar sind, geroutet werden.

Zusammen mit der Auswertung der TCP-Portnummer, die vom Terminal auf IRENE angesprochen wird, ermöglicht dies ein flexibles Nachrichtenrouting, das allen Belangen auch eines heterogenen Netzbetriebes gerecht wird.

Solche Kundenanforderungen wurden von uns bereits realisiert.

Mit keinem bekanntem Router können Sie so kundennah reagieren.

Timergesteuerte Verbindungsüberwachung

Üblicherweise wird der Verbindungsaufbau vom POS-Terminal ausgelöst, die Anfrage gesendet, das Autorisierungssystem sendet die Antwort zurück und das POS-Terminal legt auf und macht dadurch den Port für eine neue Anfrage frei. Sollte dieser normale Ablauf irgendwie gestört werden, löst das Autorisierungssystem die Verbindung nach Überschreiten einer eingegebenen Zeit die Verbindung aus und macht den Port wieder frei.

Sollte der Timer in beiden Systemen nicht ansprechen, wird als letzte Instanz der Vorrechner IRENE die Verbindung trennen. Damit haben Sie die Sicherheit, dass Ihre kostbaren TCP-Ports nicht länger als unbedingt belegt sind und danach sofort wieder für weitere Anrufe zur Verfügung stehen.

Sicherheit gegen TCP-Attacken

Wird der VPN-Verkehr über den Vorrechner IRENE geleitet, haben Sie damit geradezu ein Bollwerk gegen TCP-Attacken wie Brut Force Attack, Spoofing, DoS, SYN Flood, etc.

Alle diese Angriffe werden von IRENE aufgehalten und Ihre Hauptkomponenten bleiben von diesen Angriffen verschont.

Haben Sie zwei Vorrechner IRENE mit unterschiedlichen IP-Adressen installiert, überleben sie sogar ein totales Überfluten einer IRENE mit Spoofing Paketen.

Selbst wenn der zweite Vorrechner IRENE ebenfalls überflutet wird, werden all diese Angriffe von Ihrem Hauptsystem ferngehalten, so dass nach Beendigung der Angriffe Ihr VPN-Zugang wieder ungestört zur Verfügung steht.

Auf all diese o. a. Punkte müssten Sie verzichten, würden Sie die VPN-Daten direkt auf das Autorisierungssystem leiten!