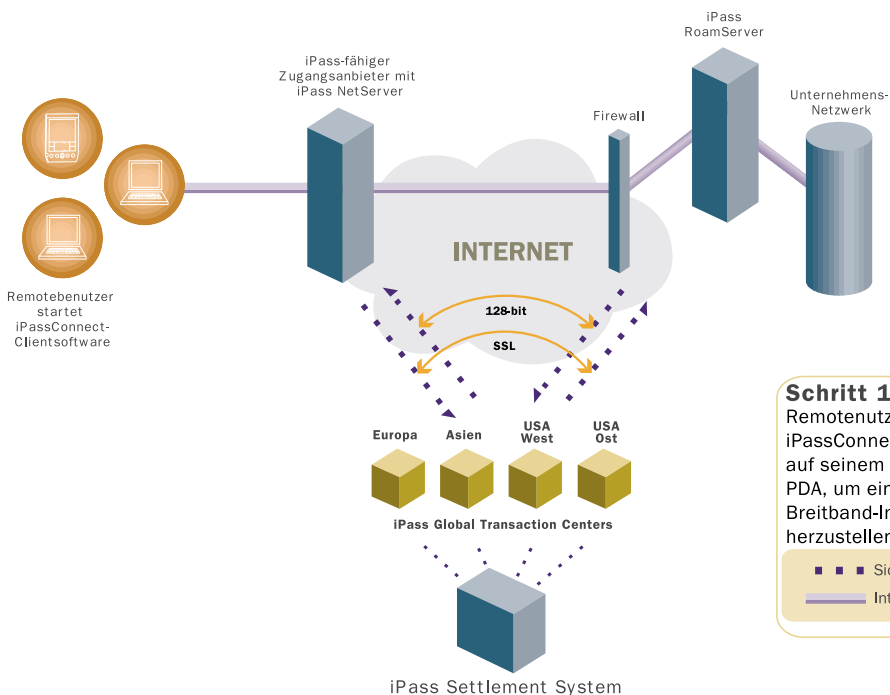


## PROBLEMLOSER, ZUVERLÄSSIGER WELTWEITER VPN-ZUGANG FÜR ROAMINGNUTZER

Das globale iPass-Netz bietet Geschäftsreisenden und Remotennutzern den zuverlässigen Zugang zu virtuellen privaten Netzen (VPN) an nahezu jedem beliebigen Ort, einschließlich Flughäfen, Kongresszentren und Hotels. Dank der redundanten Netzabdeckung

in allen wichtigen Geschäftszentren in mehr als 150 Ländern sowie der bewährten Kompatibilität mit allen führenden VPN-Clients ist der Aufbau einer iPass VPN-Verbindung so einfach wie die Anwahl einer lokalen Telefonnummer.

iPass VPN ZUGANG FÜR ROAMINGNUTZER



**Schritt 1**  
Remotennutzer startet iPassConnect Clientsoftware auf seinem Notebook oder PDA, um eine sichere Breitband-Internet-Verbindung herzustellen.

- ■ ■ Sichere Authentifizierung
- Internetverbindung

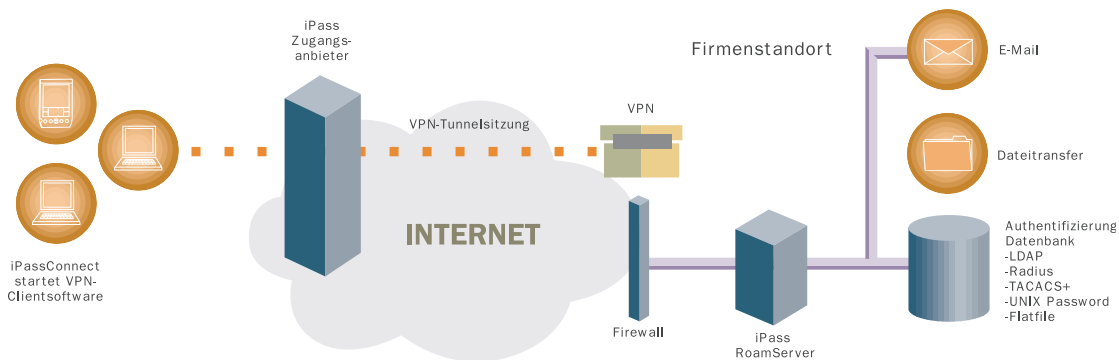
### VORTEILE

**Benutzerfreundlich**  
Zuverlässiger, redundanter weltweiter Einwahl-, ISDN- und Breitbandzugang im Festnetz

**Bewährte Kompatibilität**  
mit bekannten VPN-Architekturen

**Start über Mausclick**  
Startet mit einem einzigen Mausclick automatisch die VPN-Clientsoftware

**Höchste Sicherheit**  
Sicherheit und Datenschutz durch Übertragung aller Informationen mit 128-Bit-SSL-Verschlüsselung



### Schritt 2

Nach dem Aufbau einer sicheren Internetverbindung startet iPassConnect automatisch eine VPN-Clientsitzung. Das VPN baut einen sicheren Tunnel mit 128-bit-Verschlüsselung zwischen dem Notebook oder PDA des Nutzers und der sicheren Unternehmensnetzressource auf. Auf diese Weise erhält der Nutzer uneingeschränkten Zugriff auf Unternehmensapplikationen, Datenbanken und E-Mail-Systeme.

- ■ ■ VPN-Tunnel
- Internetverbindung



Über die branchenführende iPassConnect-Client-Software, die den Anwahlvorgang und die Initialisierung steuert und nach dem Verbindungsaufbau automatisch einen installierten VPN-Client startet, kann der mobile Nutzer weltweit auf das Internet sowie auf seine E-Mail und das firmeneigene VPN zugreifen.

Darüberhinaus leitet iPassConnect die Authentifizierungsanforderung des Roamingnutzers an den firmeneigenen Authentifizierungsserver weiter, um einen sicheren Tunnel zum Unternehmensnetzwerk aufzubauen. Auf diese Weise kann das Unternehmen ein und denselben Authentifizierungsserver sowohl für Roamingnutzer als auch für Mitarbeiter vor Ort einsetzen. Die gesamte Verbindung ist dadurch vom Anfang bis zum Ende lückenlos durch 128-Bit-SSL-Verschlüsselung geschützt.

#### INTEGRATION UND KOMPATIBILITÄT

Das iPass-Netz ermöglicht die nahtlose Integration unterschiedlichster Netztypen in eine gemeinsame Netzzugangsressource und damit die Nutzung zukunftsweisender netzübergreifender Anwendungen. Die iPass-Netzinfrastruktur und der iPassConnect-Client können in Verbindung mit einer breiten Palette von VPN-Lösungen genutzt werden:

Cisco - VPN 3000 Concentrator Series  
 Alcatel/Newbridge - Timestep PERMIT Gate  
 Certicom - movianVPN™  
 Check Point - SecuRemote  
 Indus River - Riverworks/Riverpilot  
 Intel - NetStructure VPN  
 Lucent - Brick VPN  
 Microsoft - NT Server with PPTP  
 Nortel - Contivity 1000-4000

Der iPassConnect-Client arbeitet unabhängig von der VPN Lösung und ihrer Architektur und bietet eine Vielzahl von Konfigurationsoptionen, mit deren Hilfe sich die Bedienung vereinfachen lässt. In den meisten Fällen wird der auf einem Desktop oder Laptop eingerichtete Softwareclient an einen VPN-Server angeschlossen, der die Verbindung auf Seiten eines geschützten Firmenstandorts terminiert. Der Server lässt sich je nach Netzarchitektur und allgemeinen Sicherheitsanforderungen eines Unternehmens vor, hinter oder neben einer Firewall installieren.

iPass unterhält ein VPN Solutions-Center in der kalifornischen Unternehmenszentrale, in dem die Kompatibilität der iPass-Remotezugangsdienste mit führenden VPN-Produkten getestet und demonstriert wird. Das Solutions-Center vermittelt dem Kunden alles Wissenswerte über Funktionsweise, Auswahl und erfolgreiche Implementierung umfassender und sicherer Remoteverbindungen. Außerdem dient es als Ansprechpartner, sollte bei der Einrichtung eines VPN-Netzes oder einer iPass-Remotezugangslösung durch den Kunden Probleme auftreten.

#### ZUSÄTZLICHE SICHERHEITSMABNAHMEN

iPassConnect lässt sich so konfigurieren, dass eine sichere Verbindung zwischen der VPN-Sitzung und der aktiven Internetverbindung aufgebaut wird. Zu diesem Zweck wird ein Timer eingerichtet, der den Verbindungsaufbau des Benutzers mit dem VPN-Netz überwacht. Sollte der Zugang und die Authentifizierung nicht innerhalb der festgelegten Zeit erfolgen oder eine aktive VPN-Sitzung unterbrochen werden, beendet iPassConnect die Internetverbindung automatisch.

Weitere Informationen erhalten Sie telefonisch unter der Rufnummer **+49 (0)89-54 55 81 20** oder auf der iPass-Website unter [www.ipass.com](http://www.ipass.com).



iPass EMEA

D/A/CH

Dachauer Str.37/5.0G

D-80335 München

Tel.: +49 (0)89/54 55 81 20

Fax: +49 (0)89/54 55 83 33

[www.ipass.com](http://www.ipass.com)

iPass und das iPass Logo sind Marken von iPass Inc. Alle übrigen in diesem Dokument erwähnten Marken oder Servicemarken sind Eigentum der jeweiligen Rechtsinhaber.