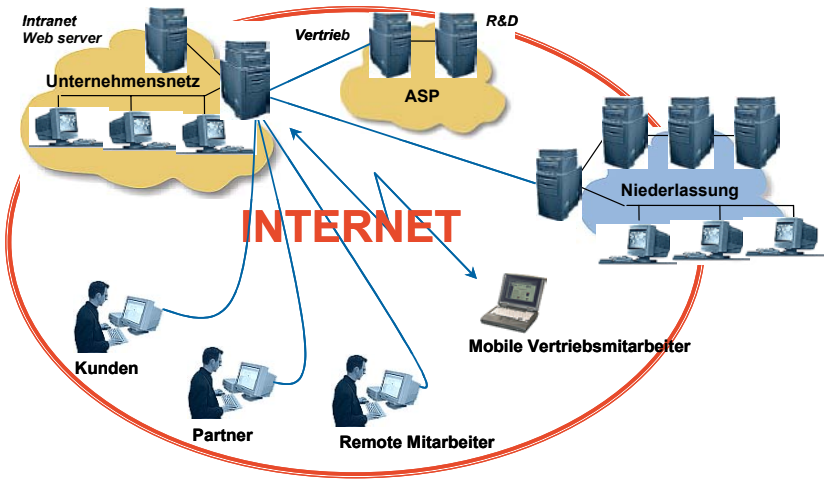
Hohe Sicherheit und tiefe Kosten – das Ziel eines jeden Unternehmens

Virtual Private Networks (VPN) helfen Ihnen Kosten zu sparen

Viele Firmen möchten ihren Mitarbeitern von unterwegs oder von zu Hause sowie ihren Kunden und Partnern die Möglichkeit bieten auf das Unternehmensnetz zuzugreifen. Auch gängige B2B-Lösungen konnten nur mit einem grossen Investitions- und Betriebsaufwand sicher realisiert werden. Die bisherigen Lösungen waren teure Einwahlinfra-strukturen, die hohe Verwaltungs- und Telefonkosten zur Folge hatten oder VPN-Lösungen basierend auf sogenannten „pre-shared secrets“, die sehr aufwändig in der Verwaltung sind und vergleichsweise mit digitalen Zertifikaten als unsicherer zu betrachten sind.



Was ist VPN

Virtual Private Networks ist ein Überbegriff für alle Technologien, die sichere Kommunikation über unsichere Netzwerke erlauben. VPN setzt sogenannte IPSec-Tunnel zwischen zwei Gateways ein um private Daten zwischen unsicheren Netzwerken sowie das Internet zu schützen

IPSec

Das Protokoll Internet Protocol Securtiy (IPSec) wurde von der internationalen Internet Engi-neering Task Force (IETF) entwickelt und stellt Sicher-heitsservices auf Netzwerkebene zur Verfügung. Ein IPSec Tunnel über das Internet schützt den gesamten Datenverkehr unab-hängig von der Applikation.

VPN User Identifizierung

Ein VPN schützt die Integrität und Vertraulichkeit einer

Information über unsichere Netzwerke mittels Verschlüsselung. IPSec selbst sieht keine Identifizierung des Endbenutzers vor. Hier kommen nun digitale Zertifikate zur sicheren Identifizierung zur Anwendung: Digitale Zertifikate und Public Key Infrastrukturen sind bei weitgehend allen namhaften Herstellern als Identifikationsmittel integriert.

VPN Typen

Virtual Privat Networks können für Client zu LAN, LAN zu LAN und Extranet zu VPN für Kunden, Partnerfirmen und Lieferanten eingesetzt werden.
Digitale Zertifikate werden deshalb nicht nur für Personen sondern auch für Applikationen oder Server eingesetzt. Eine Trusted Third Party wie SwissCERT garantiert die Identität der Server oder Personen. So kann, basierend auf Public-Key-Kryptographie, die sichere Authentifizierung des VPN-Entpunktes oder der Person sichergestellt werden.

Kosteneinsparung

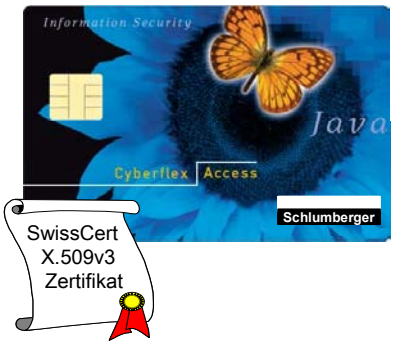
Die Kommunikationskosten für kleinere Netzwerke lassen sich in der Regel um ca. 20 bis 40 Prozent senken, bei grösseren, internationalen Netzwerken sind die Einsparungen sogar höher.

Einsparungen bei den Administrationskosten zur Unterstützung von Remote Access Lösungen lassen sich ebenfalls um beeindruckende 50 bis 70 Prozent senken.

Die Lösung

Das modulare Security Add-on Package von Schlumberger, SwissCERT und IT-Secure.com AG basiert auf digitalen Zertifikaten, die auf einem Hardwaretoken (SmartCard) sicher gespeichert sind. Dies ergänzt eine Standard VPN Lösung zu einer sicheren und effizienten Gesamtlösung.

Der Betrieb der Public Key Infrastruktur wird durch SwissCERT wahrgenommen. Benutzernamen und Passwort werden durch einen PIN Code und einem auf einem Hardwaretoken gespeichertem Zertifikat ersetzt. Dies ist für den Benutzer eine absolut transparente Lösung, die einfach zu verwalten ist und Ihre Infrastrukturkosten gegenüber herkömmlichen Lösungen deutlich senkt.



SwissCert AG
Rümlangerstrasse 9
CH-8105 Watt
Tel: +41 (0)43- 344 55 27
Fax: +41 (0)43- 344 55 28
e-mail: info@swisscert.com

LHS AG, Member of Schlumberger
Binzmühlestrasse 95
CH-8050 Zürich
Tel: +41 (0)1- 308 95 10
Fax: +41 (0)1- 308 95 99
e-mail:

IT-Secure.com AG
Rümlangerstrasse 9
CH-8105 Watt
Tel: +41 (0)43- 411 81 02
Fax: +41 (0)43- 411 81 02
e-mail: info@it-secure.com

Key Features

- *Starke Authentifizierung basierend auf digitalen Zertifikaten*
- *UBS-Token oder SmartCard als Speichermedium*
- *Starke Verschlüsselung*
- *Einfacher Rollout*
- *Webbasiertes Administrations-GUI*

Vorteile

- *Vertraulichkeit und Integrität der Daten wird sichergestellt*
- *Teuere Standleitungen oder Dial-in Infrastruktur nicht mehr notwendig für Remote Zugriff*
- *Sämtliche Applikationen werden unterstützt*
- *Sichere Identifikation Ihrer Kunden, Partner oder Mitarbeiter*
- *Nahtlose Ergänzung zur existierenden Sicherheitsinfrastruktur*
- *Problemlos erweiterbar für Secure E-Mail*
- *Problemlos erweiterbar für Secure Single Sign on*
- *Problemlos erweiterbar für Microsoft Logon basierend auf digitalen Zertifikaten und SmartCards*

Kompatible Produkte

- *Checkpoint FW1*
- *Cisco*
- *Sonicwall*
- *und viele mehr ...*