

Inhaltsverzeichnis

1. DEFINITION	1
2. KONNEKTIVITÄT	2
3. STANDARDS	2
4. ANWENDUNGSBEISPIELE	3
5. VPN ALS SERVICE	5
6. EMPFEHLUNGEN	6

Summary

Der Artikel gibt eine Definition von *VPN* auf der IP-Ebene und zeigt die heute populärsten Konnektivitätstypen *RAS*, *Intranet-Intranet* und *Intranet-Extranet* auf die mit entsprechenden Anwendungsbeispielen ergänzt sind. Die weitgehend anerkannten Sicherheitsstandards *IPSec* und *PKI*, welche für *VPN* eine zentrale Bedeutung haben, werden kurz skizziert. In einem Überblick wird der heutige Stand des *VPN*-Anbieter-Marktes der Schweiz, an einigen ausgewählten Beispielen, aufgezeigt.

1. Definition

Es ist festzustellen, dass besonders im „IP-Marktsegment“ in den letzten Jahren die Sicherheits-Technologie- bzw. Sicherheits-Ausrüstungsbereiche enorme Entwicklungen geleistet haben. Dies hat damit zu tun, dass das *Internet* von Wirtschaft und Gesellschaft als *das* (globale) Netz entdeckt wurde und heute vermehrt für geschäftskritische Anwendungen, mit hohen und teilweise sehr hohen Anforderungen an die Sicherheit (z.B. *Internet* für Business-to-Business Anwendungen), eingesetzt wird. Unter diesen Aspekten ist VPN (virtual private network) heute zu sehen.

Damit ist auch gesagt, dass sich die nachfolgende Beschreibung bewusst auf die Darstellung der IP-Ebene beschränkt. In wie weit untere Kommunikationsebenen (Layer 2, z.B. ATM) von weiteren Sicherheitsüberlegungen, um z.B. Routing-Attacken (Modifikation der ATM-Zellenheader) o.ä. entgegenzuwirken, betroffen sind, ist abhängig von den Sicherheitsanforderungen des Anwenders eines VPN. In der Regel sind für diese Fälle die Carrier/Provider, als Betreiber der weitreichenden Übertragungs-Basisinfrastrukturen, angesprochen.

Ein VPN (virtual private network) gilt als ein sicheres Telekommunikationsnetz obwohl verschiedene, voneinander unabhängige Benutzerorganisationen, z.B. von multinationalen Grossfirmen bis hin zu KMU, die gleiche öffentliche Netzinfrastruktur nutzen (shared network oder public network). Die Architektur heutiger VPN basiert wie oben erwähnt, primär auf den TCP/IP Protokollen.

Der Unterschied zwischen konventionellen Netzen und VPN liegt in der virtuellen bzw. logischen Sicht des Netzes. Die Datenpakete werden vor der Übermittlung über VPN authentisiert und chiffriert (*Kapitel 3*). Das damit erzeugte „secure tunneling“ gewährleistet die Sicherheit, d.h. Authentizität, Vertraulichkeit und Integrität der Daten, die gleichzeitig von verschiedenen Benutzergruppierungen übertragen werden.

Durch „secure tunneling“ entsteht die Charakteristik eines privaten Netzes, welches wesentlich flexibler und somit kostengünstiger betrieben werden kann, als ein privates Netz, das aus dedizierten, statischen Mietleitungen aufgebaut ist.

Für Benutzer eines VPN spielt es keine Rolle ob sie sich, zur Realisierung eines Intra- oder Extranets mittels der nachfolgend beschriebenen VPN-Mechanismen, an den *IP-Backbone* eines Carriers oder an das *Internet*, via Internet-Access-Provider, anschliessen.

Benutzer eines VPN können Telekommunikationsservices wie z.B. E-Mail, Filetransfers, Client/Server Transaktionen, Telefonie, Video/Audio etc., wie sonst üblich nutzen. Sie merken nichts davon, dass ihre IP-Datenpakete authentisiert und chiffriert übertragen werden und dadurch vor möglichen Angriffen (z.B. aktives oder passives Abhören der Kommunikation, Modifikation von Daten, Maskerade etc.) dritter Netzbenutzer oder der Netz-Betriebsorganisation des Providers weitgehend geschützt sind. Zusätzlich können die Sicherheitsverfahren stichhaltige Beweise zu Ursprung, Sendung oder Empfang der Daten leisten.

2. Konnektivität

Wichtig ist, für mittlere oder grössere Unternehmen und Organisationen zu erkennen, dass in komplexen Netzen in der Regel alle nachfolgend aufgezeigten Konnektivitätstypen gleichzeitig vorkommen. Dies führt zum Schluss, dass nur eine VPN-Lösung die auf anerkannten Sicherheitsstandards aufbaut, langfristig erfolgreich und ökonomisch eingesetzt werden kann.

Bei der nachfolgenden Differenzierung kann vom *Intranet* als Voraussetzung für die interne Kommunikation ausgegangen werden.

- Secure Remote access (RAS)** - RAS ist für die sichere Kommunikation für Mitarbeiter des Unternehmens im Aussendienst von unterwegs oder von privaten Stellen aus vorgesehen.
- Secure Intranet – Intranet** - Intranet – Intranet Verbindungen sind das geeignete Mittel für den Verbund weiterer Neben- oder Zweigstellen eines geographisch dezentralen Unternehmens.
- Secure Intranet – Extranet** - Intranet – Extranet Verbindungen dienen für den Verbund des Unternehmens mit verschiedenen, voneinander unabhängigen Geschäftspartnern, z.B. für den Austausch vertraulicher Geschäftsdokumente.

3. Standards

IPSec:

Der heute in IP-Netzen am weitesten verbreitete und anerkannte VPN-Sicherheitsstandard ist IPSec¹. IPSec wurde von der IETF (Internet Engineering Task Force) übernommen und grösstenteils verabschiedet.

IPSec umfasst eine Sammlung von Normen (RFC, Request for comment) welche die Vertraulichkeit, Integrität und Authentizität von IP-Daten sowie die Zugangskontrolle für Benutzer regeln. Ebenfalls werden mit IPSec die Verfahren für die Chiffrierung und den Austausch der notwendigen Chiffrier-Schlüssel festgelegt.

Eine Auswahl aus den Normen der IETF für IPSec sind nachfolgend aufgelistet:

- Security Architecture for the Internet Protocol RFC 2401
- IP Authentication Header RFC 2402
- IP Encapsulating Security Payload (ESP) RFC 2406
- Internet Security Association and Key Management Protocol (ISAKMP) RFC 2408
- The Internet Key Exchange (IKE) RFC 2409

¹ IPSec: Internet Protocol Security. Andere (proprietäre) Protokolle haben sich nicht durchgesetzt, z.B. Point to Point Tunneling Protocol (PPTP (Layer 2), bettet PPP frames in IP Datagramme ein).

Im Bereich „IPSec für remote access“ besteht heute ein Entwurf (draft-ietf-ipsra-reqmts-00.txt, März 2000). Die vollständige IPSec Normensammlung mit detaillierten Angaben zu Funktionsweisen und weitere Einzelheiten zum Thema IPSec befinden sich unter <http://www.ietf.org/html.charters/ipsec-charter.html>.

PKI:

Die Public-Key-Infrastructure (PKI) dient zur Authentisierung von Benutzern (oder Instanzen) eines VPN². PKI ist besonders für ausgedehnte VPN geeignet, insbesondere für extensive RAS- oder Extranet-Anwendungen. PKI stellt das Management der digitalen Zertifikate und Chiffrier-Schlüssel sicher.

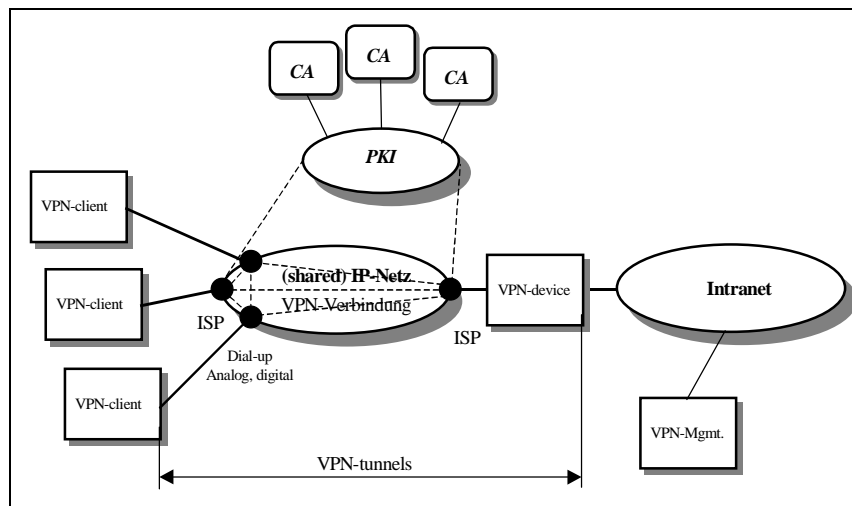
Die Sicherheits-Verfahren der PKI eignen sich ausser für VPN auch für andere Internet-Anwendungen, wie zum Beispiel Web, E-Mail etc.. Die PKI gilt als aussichtsreichste Kandidatin für die Realisierung einer staatlich anerkannten, sicheren Identifizierung von Kommunikationspartnern.

Eine PKI umfasst, nebst dem Public-Key-Sicherheitsverfahren, anerkannte Vertrauensstellen (Certification Authority, CA). Die CA (Trust-Servicecenter) bescheinigt beispielsweise mit ihrer digitalen Signatur, dass ein bestimmter öffentlicher Chiffrier-Schlüssel einer bestimmten Person zugeordnet ist. Weitere Elemente einer PKI sind Verzeichnisdienste die dazu dienen, den öffentlichen Teil der Chiffrier-Schlüssel, zusammen mit Validierungsinformationen (z.B. Gültigkeitsdauer), anderen Benutzern verfügbar zu machen. Informationen zum Thema PKI in der Schweiz befinden sich unter http://www.bakom.ch/ger/subpage/?category_104.html. Die „Verordnung über Dienste elektronischer Zertifizierung“, vom 12.04.2000, kann als PDF-Datei heruntergeladen werden.

4. Anwendungsbeispiele

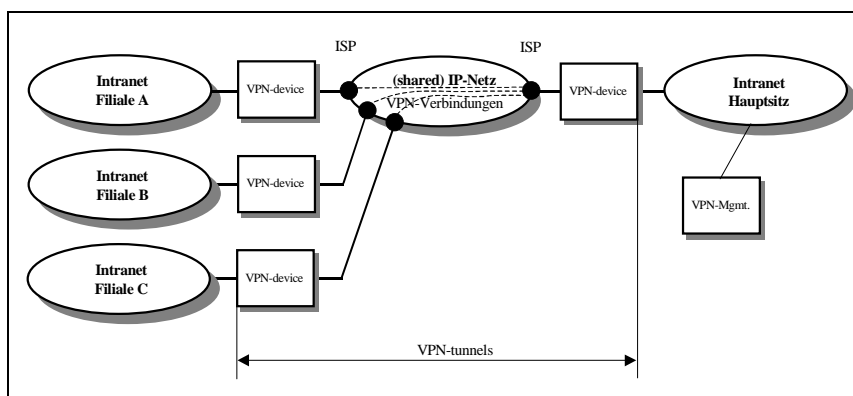
Für die Realisierung eines RAS-VPN (*Figur 1*) werden VPN-Clients mit VPN-Software auf der einen Seite und ein VPN-Device, z.B. Firewall, Router/Switch oder dedizierte VPN-Devices (Security-Box), auf der anderen Seite benötigt. Die VPN-Konfiguration wird mittels VPN-Managementconsole bzw. –Workstation verwaltet. Zwischen den VPN-clients und dem VPN-device erfolgt die Kommunikation durch die sicheren VPN-Tunnels.

² Für geeignete Authentisierungsverfahren in VPN siehe RFC 2408, 2409.



Figur 1: - Secure remote access (RAS)

Figur 2 zeigt ein unternehmensweites VPN. Ein Unternehmen kann auf diese Weise vertrauliche Geschäftsdokumente sicher über ein IP-Netz (z.B. das Internet), zwischen Hauptsitz und Filialen, austauschen. Wenn das Internet als Träger der VPN-Verbindungen gewählt wird, ist es besonders wichtig die Anforderungen in Bezug auf QoS (quality of service) des Gesamtnetzes zu definieren, da das Internet bis heute keine diesbezüglichen End-to-End QoS-Garantien bietet³. In dieser Konfiguration werden VPN-Devices, z.B. Firewalls, Router/Switches oder dedizierte Systeme (Security-Boxes) inkl. VPN-Management-System benötigt.

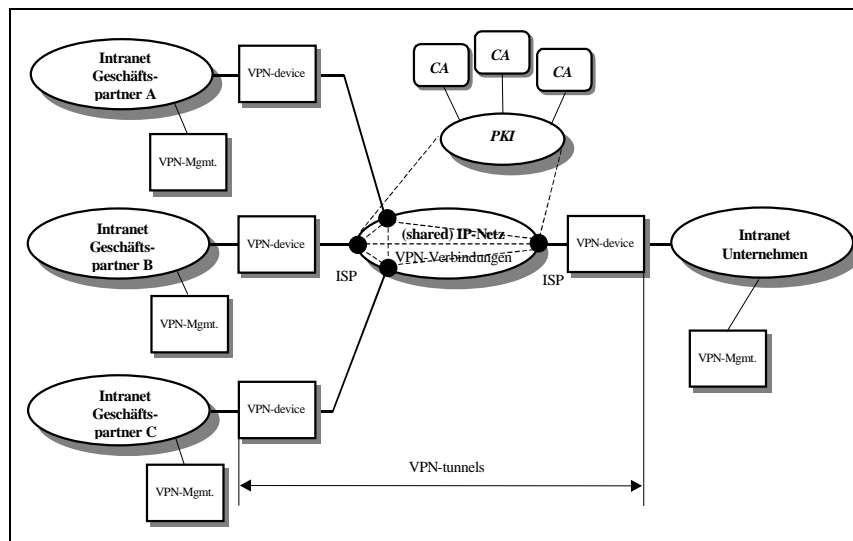


Figur 2: - Secure site-to-site Konfiguration

In Figur 3 ist ein VPN-Szenario als Extranet gezeigt, welches verschiedene, voneinander unabhängige Geschäftspartner via Internet miteinander verbindet. In dieser Konfiguration werden VPN-Devices, z.B. Firewalls, Router/Switches oder dedizierte Systeme (Security-

³ Das Internet bietet heute den jeweils bestmöglichen Service in Funktion der Belastungssituation (best-effort-service). Dies kann eine grosse Varianz der Antwortzeit zur Folge haben. Ursache sind die hohe Varianz der Warteschlangen-Verweilzeiten (buffer delays) sowie wiederholtes übermitteln verlorener Datenpakete nach Netzblockaden. Dies kann speziell bei zeitkritischen Anwendungen (IP-Telefonie) problematisch sein. Die IETF setzt zur Lösung der Problematik eine entsprechende Arbeitsgruppe ein (<http://www.ietf.org/html.charters/intserv-charter.html>).

Boxes) inkl. VPN-Management-Systeme benötigt. In diesem Fallbeispiel ist die Notwendigkeit des Einsatzes einer VPN-Lösung die auf einem anerkannten Sicherheitsstandard basiert, besonders augenfällig.



Figur 3: - Secure Extranet Konfiguration

5. VPN als Service

Verschiedene Internet-Service-Provider (ISP) in der Schweiz bieten heute VPN als Teil ihres Service-Portfolios an. Damit entfällt dem zukünftigen VPN-Nutzer die Investitionsbürde die für eine Realisierung des VPN notwendig ist. Dem Nutzer bleiben die Betriebskosten und das Management sicherheitsrelevanter Elemente (Schlüssel, Zertifikate etc.) bzw. dessen Organisation.

Nachfolgend sind die VPN-Services einiger Service-Provider in der Schweiz übersichtsmässig zusammengefasst. Detaillierte Auskünfte betreffend VPN-Lösungen können bei den ISPs direkt eingeholt werden.

Anbieter	Backbone	Bandbreiten	Security-Standards	Services	Verfügbar	Zielgruppen	SLA	HW
INFONET	Infonet	k.A.	IPSec/PKI	DialXpress Internet (RAS) IP-VPN (IPSec, MPLS) für Intra-/Extranet	3./4. Q 2000 2.Q 2001	Allgemeine Anwender Allgemeine Anwender	ja	CISCO
MCI Worldcom	UUnet	64 kb/sec – 45 Mb/sec	IPSec/PKI (DES/3DES)	UUSecure-Service	ab sofort	Allgemeine Anwender	ja	XEDIA
SUNRISE	Sunrise	64 kb/sec – 2 Mb/sec	IPSec/PKI (PPTP)	Sunrise ip vpn	ab sofort	Allgemeine Anwender, KMU	ja	Firebox II

Tabelle 1: - VPN-Services einzelner Anbieter

Zusammenfassung:

Zusammenfassend kann gesagt werden, dass alle befragten Anbieter ihre VPN-Services auf der Basis von *IPSec* aufbauen, was die eingangs gemachte Aussage betreffend hoher Anerkennung des Standards durch alle beteiligten Parteien in einem VPN-Netz, d.h. Produzenten und Benutzer des Services, bestätigt.

Unklar sind die Angebote im Bereich des VPN-managements, d.h. der sicherheitsrelevanten Elemente. Es stellt sich hier die Frage inwieweit aus der Sicht der Sicherheit der Serviceprovider oder der Kunde selber diese Aufgabe wahrnehmen soll.

6. Empfehlungen

Es sollen ausschliesslich starke Chiffrierungs- und Authentisierungs-Verfahren verwendet werden. Die Schlüssellänge (Anzahl Bit) soll optimal gewählt werden können. Sie stellt einen Kompromiss zwischen erzielbarer Sicherheit und Leistung dar. Mit *IPSec* ist dies gewährleistet.

Wie bereits erwähnt ist bei *IPSec*-Implementationen auf die Konformität in Bezug auf den *IPSec*-Standard zu achten. Insbesondere dann, wenn mit unabhängigen Geschäftspartnern sicher kommuniziert werden soll, denn in diesem Fall sind mit grosser Wahrscheinlichkeit Netzelemente verschiedener Hersteller mit *IPSec*-Funktionalität in der Netzkonfiguration vorhanden.

Ein weiterer Punkt ist die Skalierbarkeit der Lösung. Chiffrier-Algorithmen sind erfahrungsgemäss Ressourcenintensiv. Dies kann besonders bei VPN, bei denen bekanntlich die Sicherheitsvorkehrungen auf der Netzebene (IP-Ebene) getroffen werden, zu Performanceproblemen führen. Ebenfalls nimmt der Bedarf an Leistung, bei der Durchführung des automatischen Schlüsselaustausches, mit zunehmender Anzahl der Netzknoten stark zu.

Es empfiehlt sich besonders dann, wenn bestehende Ausrüstungsteile (z.B. bereits installierte Router) zusätzlich mit *IPSec*-Funktionalität aufgerüstet werden sollen, die resultierende Leistung der betroffenen Ausrüstungen vorgängig zu klären und allenfalls auf der Hardwareebene zu erweitern. Allfällige Leistungseinbussen, verursacht durch die *IPSec*-Funktionalität, sind situationsabhängig⁴. Die Situation muss mit entsprechenden Netzmanagementtools analysiert werden.

Wird VPN als Service bezogen ist der SLA (service level agreement) ein wichtiges Instrument zur Qualitätsdefinition. In diesem Dokument müssen die garantierte Netzverfügbarkeit und Antwortzeiten (roundtrip delay) unter dem Aspekt des VPN spezifiziert sein.

Das VPN-Sicherheitsmanagement soll einfach in die allenfalls bereits bestehende IT-Sicherheitsmanagement-Architektur integrierbar sein.

⁴ erhöhter Speicherbedarf für *IPSec*-Code/-Datenstrukturen, erhöhte Latenzzeiten, reduzierter Durchsatz sind zu erwarten.