DECOIT

ONLINE 2001

Extranet

VPN-Technik zum Aufbau
sicherer Unternehmensnetze

Dipl.-Ing. Kai-Oliver Detken
Senior IT Consultant, http://kai.nord.de
DECOIT- http://www.decoit.de
Düsseldorf, den 01. Februar 2001

Consultancy & Internet Technologies

© DECOIT GmbH

Inhalt

- Kurzdarstellung von DECOIT
- Definition und Abgrenzung
- Gründe für den Aufbau eines Extranet
- Anforderung
- Beurteilung der IPsec-Spezifikation
- Hersteller- und Produktlösungen
- Performance-Tests
- Zusammenfassung

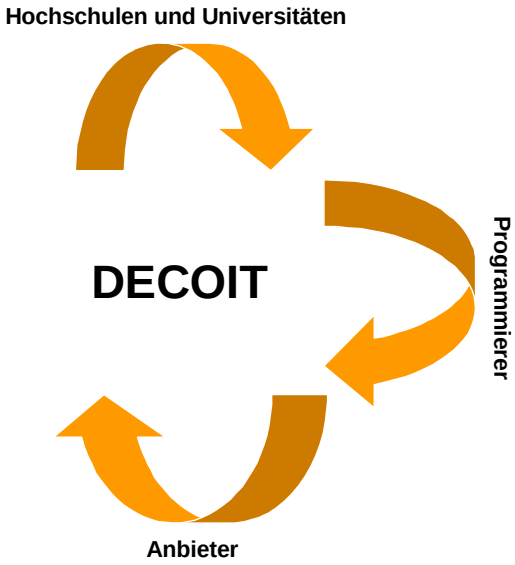
© DECOIT GmbH

Portfolio DECOIT

© DECOIT GmbH

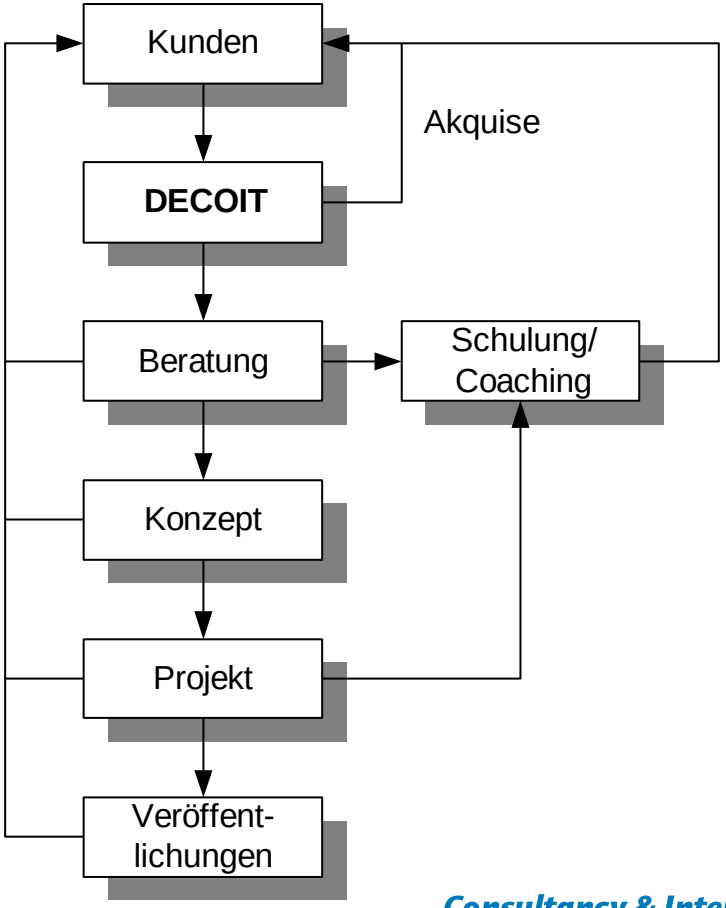
Dienstleistungsportfolio: http://www.decoit.de

- Consulting
  - Netzkonzepte
  - Sicherheitskonzepte
  - Sicherheitsüberprüfung
  - Strategiekonzepte
  - Softwarekonzepte
- Produkttests
- Förderprojekte (Forschung und Entwicklung)
- Schulungen
- Zusammenarbeit mit verschiedenen Verlagen
- Projektmanagement
- Kooperationen (Wissensnetzwerk)



© DECOIT GmbH

Zusammenspiel der Dienstleistungen



- Bündeln der Informationen
- Wissensvorsprung
- Integration neuer Technologien
- Kosten-/Nutzenanalyse
- Erkennen von Visionen, Trends und Prognosen
- Abschätzung und Evaluierung der neuesten Technologien
- Zusammenarbeit mit den führenden Herstellern
- Erkennen von Stärken/Schwächen
- Ganzheitliche Lösungen

© DECOIT GmbH

Definition und Abgrenzung

© DECOIT GmbH

Definition und Abgrenzung

- **Internet:** öffentliches weltweites Netzwerk
- **Intranet:** Benutzung von Internet-Technologien im lokalen Netz; Absicherung zum Internet hin zum Schutz der internen Daten
- **Extranet:** Anbindung von externen Systemen, z.B. Zweigstellen, Telearbeiter oder Geschäftspartner, an das lokale Netz über öffentliche Netze; Absicherung gegenüber dem Internet

© DECOIT GmbH

Marktpotenzial für Extranets

- Zentralistisch ausgerichtete Verbundorganisationen, wie beispielsweise Versicherungen, Großhandels-unternehmen, Distributoren, Zulieferer, Franchising-Unternehmen, Verbände und Vereinigungen, Logistikunternehmen, Organisationen im Gesundheitswesen, Banken, öffentliche Verwaltungen, Unternehmen im Bereich der Unikatfertigung mit dezentralen Einheiten wie beispielsweise im Schiffbau oder Anlagenbau = jedes Unternehmen
- Einsparungspotenzial von bis zu 75% (Remote Access) und bis zu 50% im Site-to-Site VPN (Quelle: NetworkWorld)

© DECOIT GmbH

Extranet-„Schichtenmodell“

Unternehmensbezogen	"Schichtenmodell" der Internet-Entwicklung	Technologiebezogen
- Vergrößerung der Marktanteil - Verbesserung des Kundenservices - Markttransparenz - Kundenbindung	**E-Commerce** Elektronische Kommunikation mit Endkunden mittels abgesicherter Kommunikationswege über das ungesicherte Medium Internet	- Content Management - sicheres Zahlungsmittel (E-Cash) - Shopping-Lösungen - Zahlungsaustausch
- effizientere Logistik der Lieferanten - schnellere Reaktionen auf den Markt - Einbeziehung der Außenstellen - Partner/Kooperationen	**Extranet** Elektronische Kommunikation mit Partnern und Lieferanten innerhalb eines Unternehmens über das Medium Internet mittels Internet-Technologie	- Sicherer Kommunikation - Electronic Data Interchange (EDI) - externe Kommunikation - Kooperationen
- Zusatzinformationen - schlankere Organisation - verbesserter Informationsfluß - schnellere Marteinführung	**Intranet** Elektronische Kommunikation innerhalb eines Unternehmens über das eigene LAN mittels Internet-Technologie	- Firmen-Teams - Internet-Dienste - interne Kommunikation - effiziente Kommunikationsprozesse

© DECOIT GmbH

Definition eines VPNs

- Bei einem VPN werden die Dienstleistungen für eine geschlossene Benutzergruppe auf der Basis eines öffentlichen Netzes so erbracht, dass sie wie die eines privaten Netzes erscheinen.
- VPNs werden häufig ausschließlich als Realisierungsform von Corporate Networks großer Unternehmen angesehen. Sie sind jedoch auch für Dienstleistungen an kleinere Gruppen (z.B. an Privatkunden) vermarktbar.

© DECOIT GmbH

Gründe für den Aufbau eines Extranet

© DECOIT GmbH

Gründe, Teil 1

- **Flexibilität eines Unternehmens:** welches nun in der Lage ist, Kundenanfragen und Kundenwünsche schneller, effizienter und globaler abzudecken, als dies bislang der Fall war. Dabei stellt ein wichtiger Punkt die mögliche Sicherheit einer solchen logischen Infrastruktur dar, weil die Kommunikation immerhin über ein ungesichertes Netz stattfindet.
- **Integration von Sprache und Daten:** wird zunehmend den IuK-Markt beherrschen.
- **Mobilität: steht** stark im Vordergrund. Der Teilnehmer möchte nicht mehr zwischen dem Fest- und Mobilfunknetz unterscheiden, wenn er auf die Unternehmensdaten oder Dienste und Applikationen zugreift.

© DECOIT GmbH

Gründe, Teil 2

- **Transparenz und Kosteneffizienz:** muss berücksichtigt werden. Um dies zu erfüllen muss ein geeignetes Accounting und Billing implementiert werden, dass genaue Abrechnungen zulässt bzw. die eigenen Kosten ständig überprüft.
- **Offenes System:** en Extranet muss als offenes System realisiert werden, welches zukünftige Entwicklungen berücksichtigt. Da momentan der Schwerpunkt klar auf dem Internetprotokoll (IP) liegt, ist der Einsatz von TCP/IP als Quasistandard zu bezeichnen. Hier werden auch zukünftig Entwicklungen stark vorangetrieben, um das Internet als Dienst-Integrationsplattform zu etablieren.

© DECOIT GmbH

Wachstum des Marktes

- Dataquest Marktstudie Dienstumsätze
  - 1999: ca. 175 Mio. DM
  - 2000: ca. 269 Mio. DM
  - 2001: ca. 377 Mio. DM
  - 2002: ca. 489 Mio. DM
- Fazit der Studie: bekannte Dienste werden auf alternativen Plattformen eingesetzt und neue, kombinierte Multimedia-Dienste wie Videokonferenzen, E-Mail über das Handy, IP-Telephonie, LAN-LAN-Verbindungen, Homebanking, Telelearning, Multimedia-Service und Shopping werden verfügbar sein.

© DECOIT GmbH

Anforderungen

© DECOIT GmbH

DECOIT

Anforderungen, Teil 1

- Verfügbarkeit
  - 7 x 24 Stunden pro Woche
  - keine Wartezeiten beim Verbindungsaufbau
- Zuverlässigkeit
  - keine Verbindungsabbrüche
- Sicherheit
  - Verhinderung der Nutzung durch Unbefugte
  - Effektiver Schutz der übertragenen Daten vor Spionage
  - Sicherstellen der Integrität und Authentifizierung
  - Schutz vor Denial-of-Service Attacken

© DECOIT GmbH

Anforderungen, Teil 2

- Performance
  - Erreichen eines Nettodurchsatzes von mindestens 75% der Bruttoübertragungsbandbreite im Mittel
- Transparenz
  - Alle Anwendungen funktionieren so, als ob eine direkte Anbindung ans Firmennetz vorliegen würde
  - TCP/IP muss in jedem Fall; IPX, SNA etc. kann unterstützt werden
- Kosteneffizienz
  - Effektives Kosten-/Nutzenverhältnis

© DECOIT GmbH

IPsec – der gemeinsame Nenner

© DECOIT GmbH

IPsec (RFC-2401)

- IPsec wurde 1998 von der IETF vorgelegt und ist ein globaler Standard
- Authentifizierung und Verschlüsselung wurden in diesem Standard festgelegt
- Zusammenwirken von Authentification Header (AH), Encapsulated Security Payload (ESP) und Key Management wird festgelegt
- IPsec setzt auf der Netzwerkschicht auf
- Vorteil von IPsec ist die breite Unterstützung in der Industrie

© DECOIT GmbH

Eigenschaften von IPsec

- **Integrität:** Die Daten können vor Verfälschung während des Transports geschützt werden, indem eine verschlüsselte Prüfsumme in das Datenpaket eingefügt wird, die der Empfänger wiederum verifizieren kann.
- **Authentizität:** Die Authentizität des Datagramms wird dadurch garantiert, dass die Integritätsbedingung auch auf die Absenderadresse zutrifft.
- **Vertraulichkeit:** Die zu transportierenden Daten können mit Hilfe eines kryptographischen Verfahrens geschützt werden

© DECOIT GmbH

...weitere Eigenschaften

- Die reine Datenübertragung wird geschützt. Daten auf der Client-/Server-Seite bleiben unverschlüsselt
- IPsec arbeitet unabhängig von jeder Anwendung und deren Verschlüsslungsmethoden
- Schutz der Daten auf den Rechnern muss durch Anwendungsprogramme sichergestellt werden
- IPsec ist in der Lage VPNs zu realisieren
- Unterteilung in Access VPNs, Intranet VPNs und Extranet VPNs

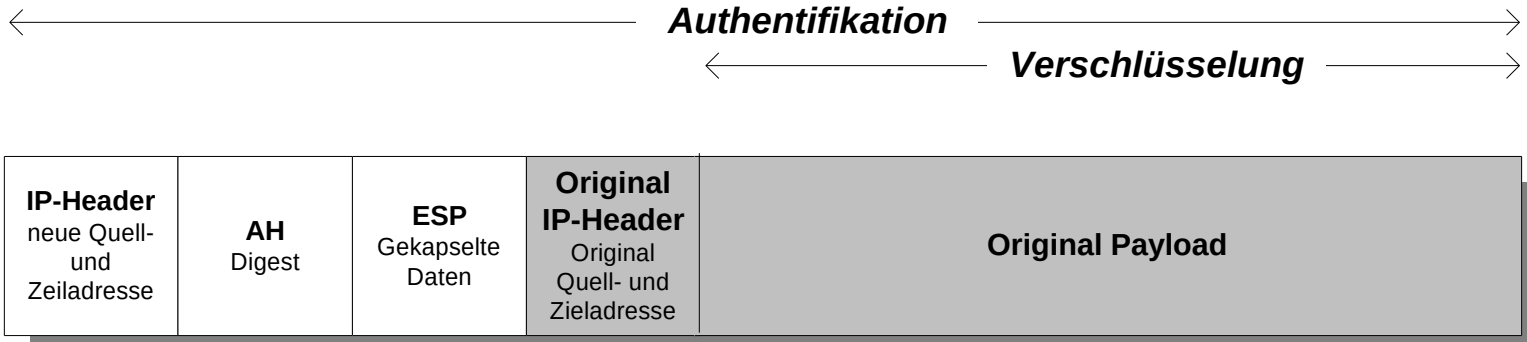
© DECOIT GmbH

Tunnel/Transport Mode

- Tunnel Mode ermöglicht die sichere Datenübertragung von IP-Paketen in IPsec-Paketen, durch Original-IP-Header
- Transport Mode für die direkte Unterstützung von IPsec
- Unabhängigkeit von der IP-Version (IPv4, IPv6)
- Symmetrische Verschlüsselung (IDEA, DES, Triple-DES) ist notwendig

© DECOIT GmbH

IPsec Header



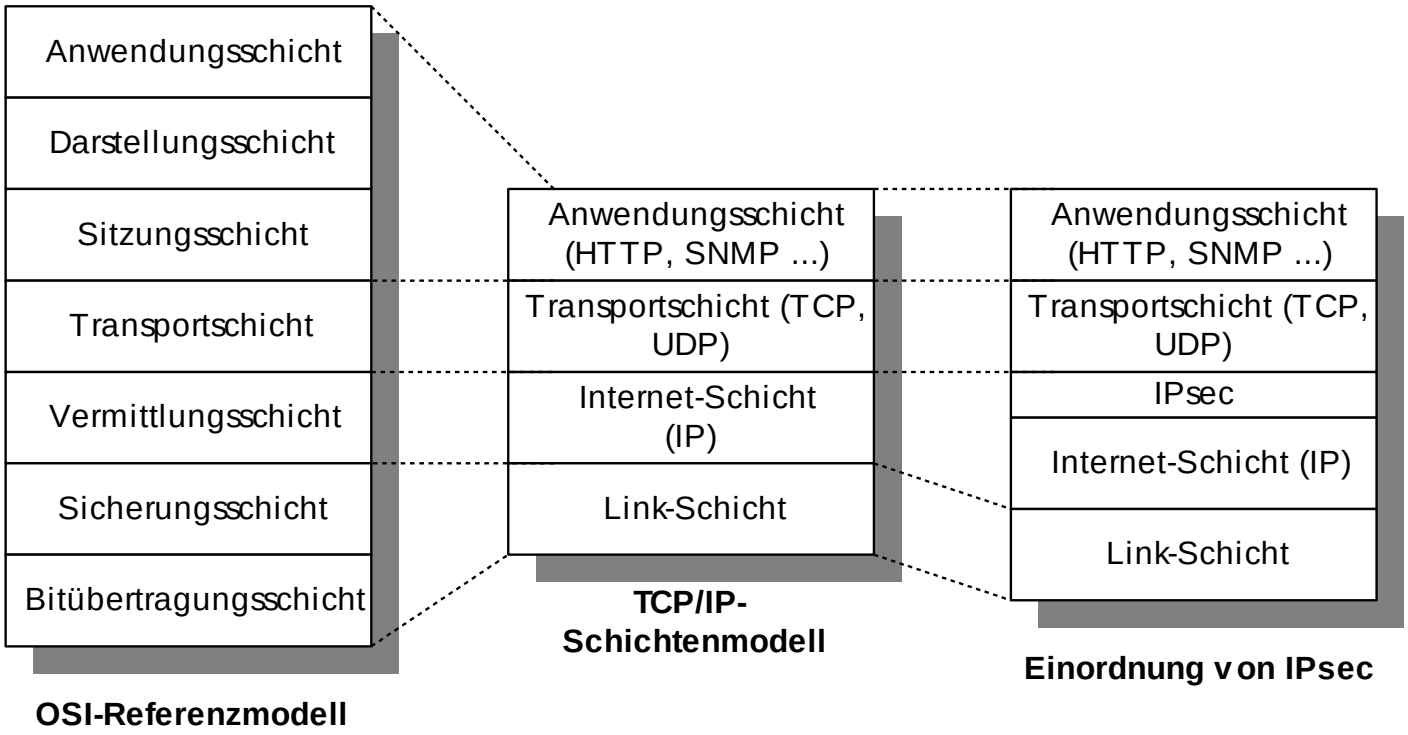
© DECOIT GmbH

Implementierungsmöglichkeiten

- **Oberhalb der IP-Schicht:** Bei Wahl dieser Methode muß der Sourcecode der logischen Schnittstelle zwischen TCP und IP verfügbar sein. Außerdem ist nur ESP möglich, da die IPsec Pakete logisch durch die IP-Schicht getunnelt werden müssen, was bei AH nicht möglich ist.
- **Innerhalb der IP-Schicht:** Dies ist besonders performance-mäßig die beste Lösung, da der Treiber der IP-Schicht ideal um IPsec-Funktionalität erweitert werden kann. Allerdings ist hierbei selbstverständlich der Sourcecode der IP-Schicht nötig.
- **Unterhalb der IP-Schicht:** Mit dieser Methode macht man die IPsec-Implementierung unabhängig vom TCP/IP-Protokollstack, allerdings ist es hierbei nötig, Fragmentierung und IP-Checksummenbildung neu zu integrieren

© DECOIT GmbH

IPsec im Schichtenmodell



© DECOIT GmbH

Key-Management

- Der IPsec-Standard wird ergänzt durch zwei Substandards:
  - SKIP - Simple Key management for Internet Protocol
  - ISAKMP - Internet Security Association and Key Management Protocol / IKE - Internet Key Exchange (IKE)

© DECOIT GmbH

VPN-Szenarien

© DECOIT GmbH

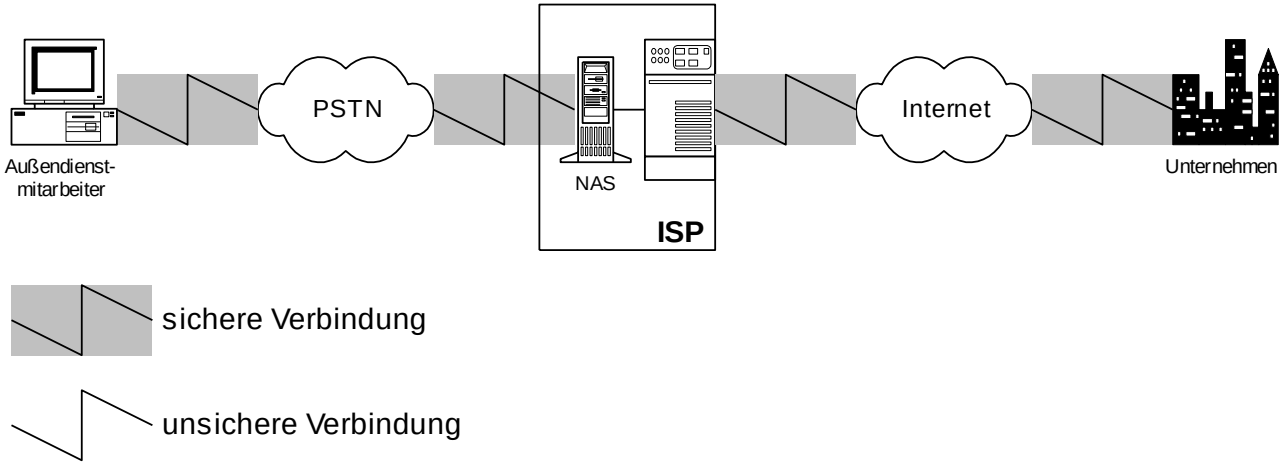
VPN-Szenarien

1. In einem Access VPN wird einer Person der entfernte Zugriff auf ein privates Netzwerk ermöglicht. So können beispielsweise Außendienstmitarbeiter auf ein Unternehmensnetzwerk sicher zugreifen.
2. Ein Intranet VPN dient dazu, den Hauptsitz eines Unternehmens und dessen privates Netzwerk mit Außenstellen zu verbinden. Dabei kann die Sicherheit der Verbindung durch Einsatz entsprechender Router gewährleistet werden.
3. Im Gegensatz zum Intranet VPN bietet ein Unternehmen im Extranet VPN zusätzlich zu den Außenstellen auch Kunden, Lieferanten und Geschäftspartnern beschränkten Zugriff auf das Unternehmensnetzwerk. In diesem Fall ist ein kombinierter Einsatz von geeigneter Hard- und Software nötig.

© DECOIT GmbH

Verbindungsaufbau, Teil 1

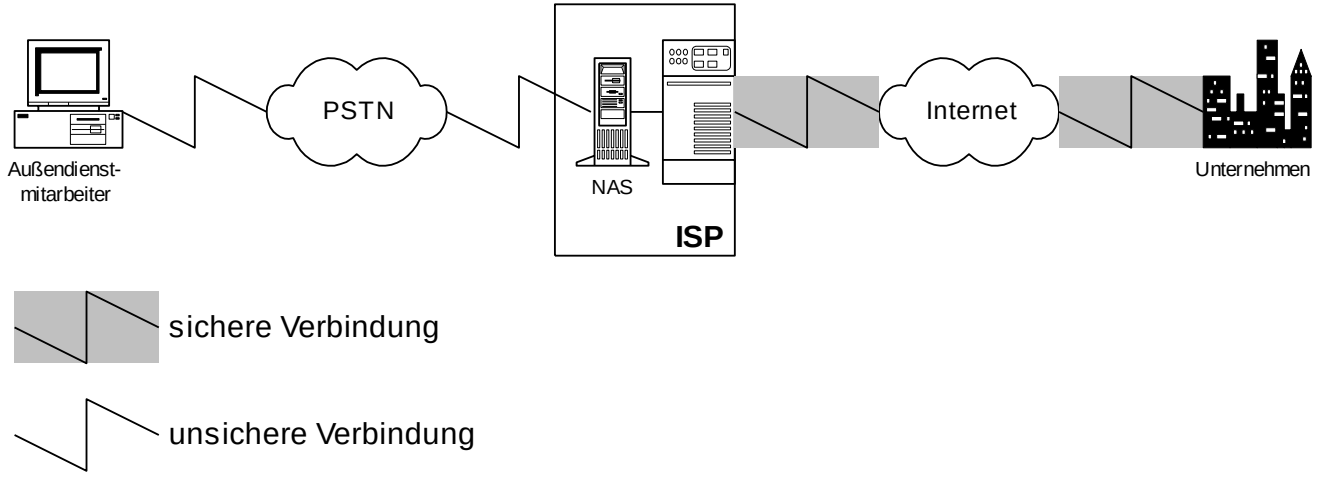
Client-initiated: Durch die Einwahlsoftware des Client-Rechners wird eine sichere IP-Verbindung zum Internet Service Provider (ISP) aufgebaut und so bis in das Unternehmensnetzwerk weitergeleitet



© DECOIT GmbH

Verbindungsaufbau, Teil 2

- **RAS-initiated:** Vom Client-Rechner wird eine nicht sichere Verbindung zum ISP aufgebaut und erst der Remote Access Server (RAS) stellt eine sichere Verbindung bis zum Unternehmensnetzwerk her



© DECOIT GmbH

Hersteller- und Produktlösungen

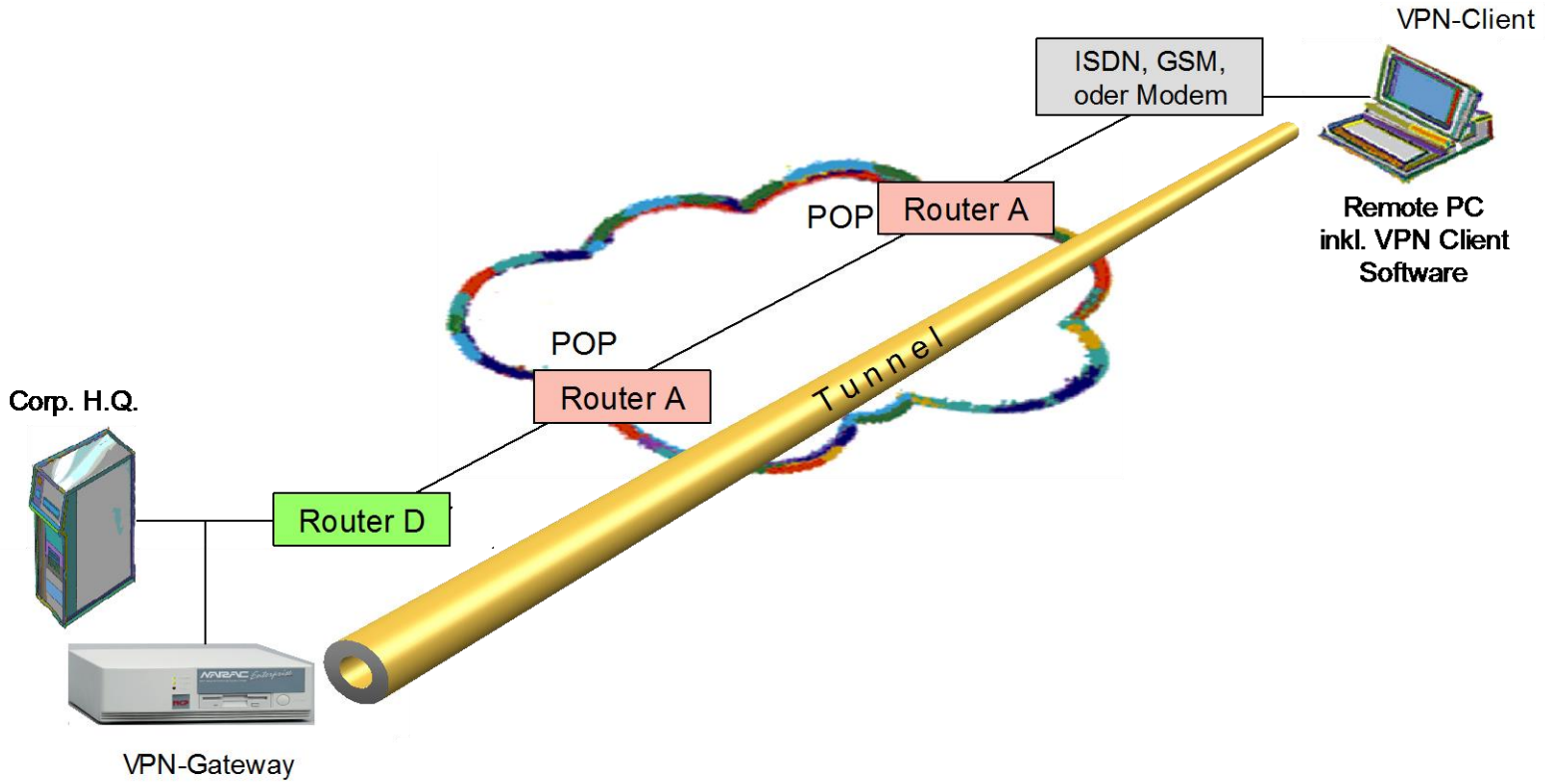
© DECOIT GmbH

NCP: High Security Remote Access Software

- Zentrale Seite
  - Network Access Server mit Standard Security (CHAP, NAT, CLI, CUG, Call Back, TripleDES, Blowfish, RSA)
  - VPN-Server mit Advanced Security (L2F, L2TP, L2sec, IPsec, SSL, PPP)
  - PKI-Server mit Strong Security (Zertifikate, digitale Signatur, SmartCards, PKI)
- Client Seite
  - Security-Client mit Standard Security (CHAP, NAT, CLI, CUG, Call Back, TripleDES, Blowfish, RSA)
  - VPN-Client mit Advanced Security (L2F, L2TP, L2sec, IPsec, SSL, PPP)
  - PKI-Client mit Strong Security (Zertifikate, digitale Signatur, SmartCards, PKI)

© DECOIT GmbH

End-to-end Tunneling



© DECOIT GmbH

Firewall-1 von Checkpoint

- **VPN-1-Gateway:** Softwarelösung, die FireWall-1 und die VPN-Technologie miteinander verbindet.
- **VPN-1-RemoteLink:** Hard- und Softwarelösung, die die Einrichtung eines sicheren Internetzugangs für Außenstellen oder Zweigniederlassungen ermöglicht.
- **VPN-1-SecuRemote:** Client-basierte Verschlüsselungssoftware, die VPN-Funktionalitäten auch für Einzelrechner, Remote- und Mobilbenutzer ermöglicht.

© DECOIT GmbH

Firewall-1, Teil 2

- **VPN-1-Certificate-Manager:** Public Key Infrastructure (PKI) System für den Einsatz öffentlicher Schlüssel. Es arbeitet zusammen mit PKI-Zertifikatsausstellern und LDAP-Verzeichnisdiensten und beinhaltet eine zentrale Policy-basierte Verwaltung. Die Authentifizierung wird mit digitalen Zertifikaten nach X.509 zwischen den Servern und den Clients unterstützt.
- **VPN-1-Accelerator-Card:** Durch diese Hardware-PCI-Karte für Sun Solaris oder Windows NT lässt sich die Performance der Datenverschlüsselung auf bis zu 45 MBit/s beschleunigen
- **Bandbreitenmanagement:** zur effizienten Ausnutzung der Ressourcen

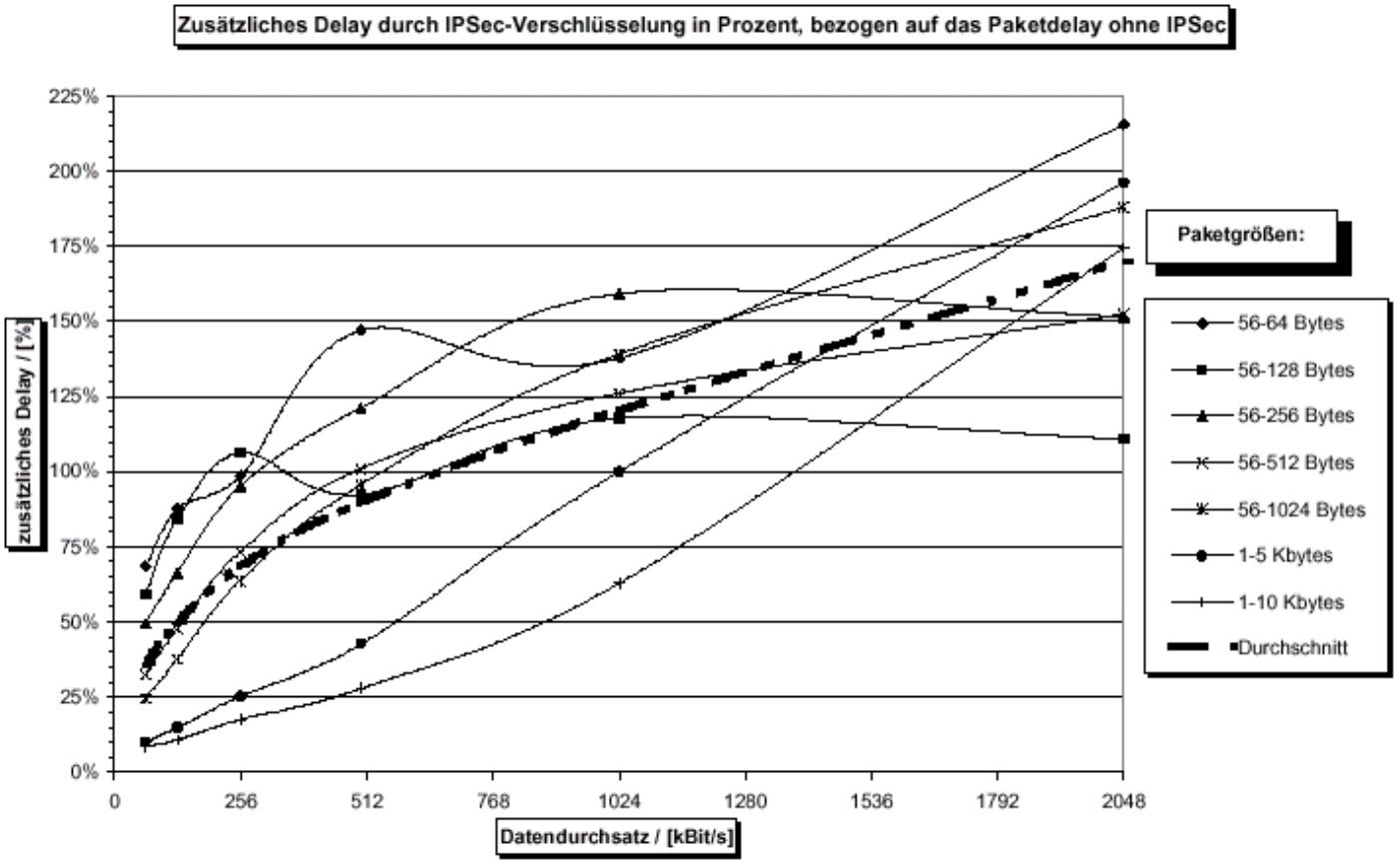
© DECOIT GmbH

Performance-Tests

- Router-Performance
  - Cisco Router 2600
  - Cisco Router 3600
- Firewall-1-Test:
  - Pentium III
  - 500 MHz
  - Windows NT
- NCP
  - Pentium II
  - 400 MHz
  - Windows NT

© DECOIT GmbH

Router-Performance



© DECOIT GmbH

Testparameter Firewall-1

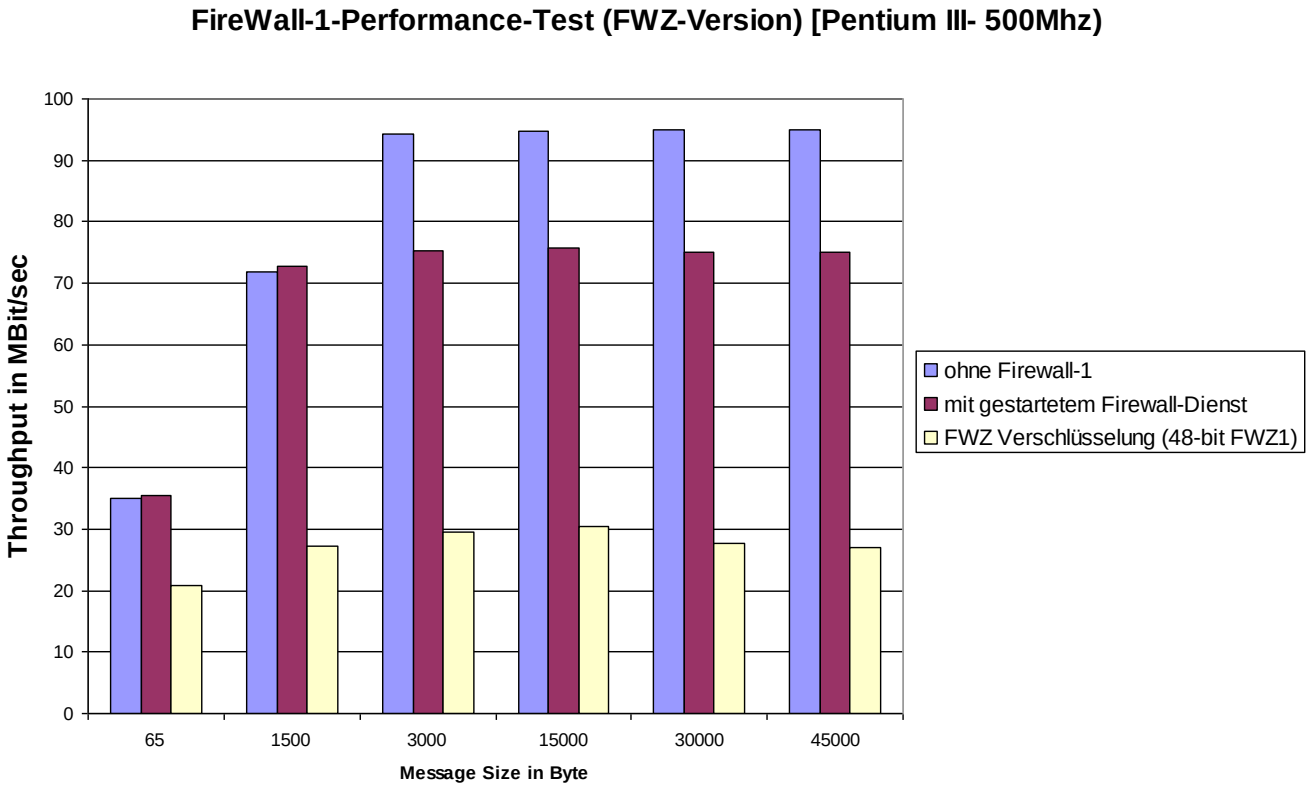
- Security Policy

No.	Source	Destination	Ser-vice	Action	Track	Install On	Time
1	Remote-User@any	Server	Any	Client Encrypt	Long	Gateways	Any
2	Any	Server	Any	Accept	Long	Gateways	Any
3	Server	Any	Any	Accept	Long	Gateways	Any

- 48-Bit-Verschlüsselung
- SecuRemote Client und die Firewall-1 verwendet
- Bei der Konfiguration der FireWall-1 wurde zuerst der Remote User 1 eingerichtet. Anschließend darf der User 1 von jeder Lokation auf die Firewall zugreifen.

© DECOIT GmbH

Firewall-1



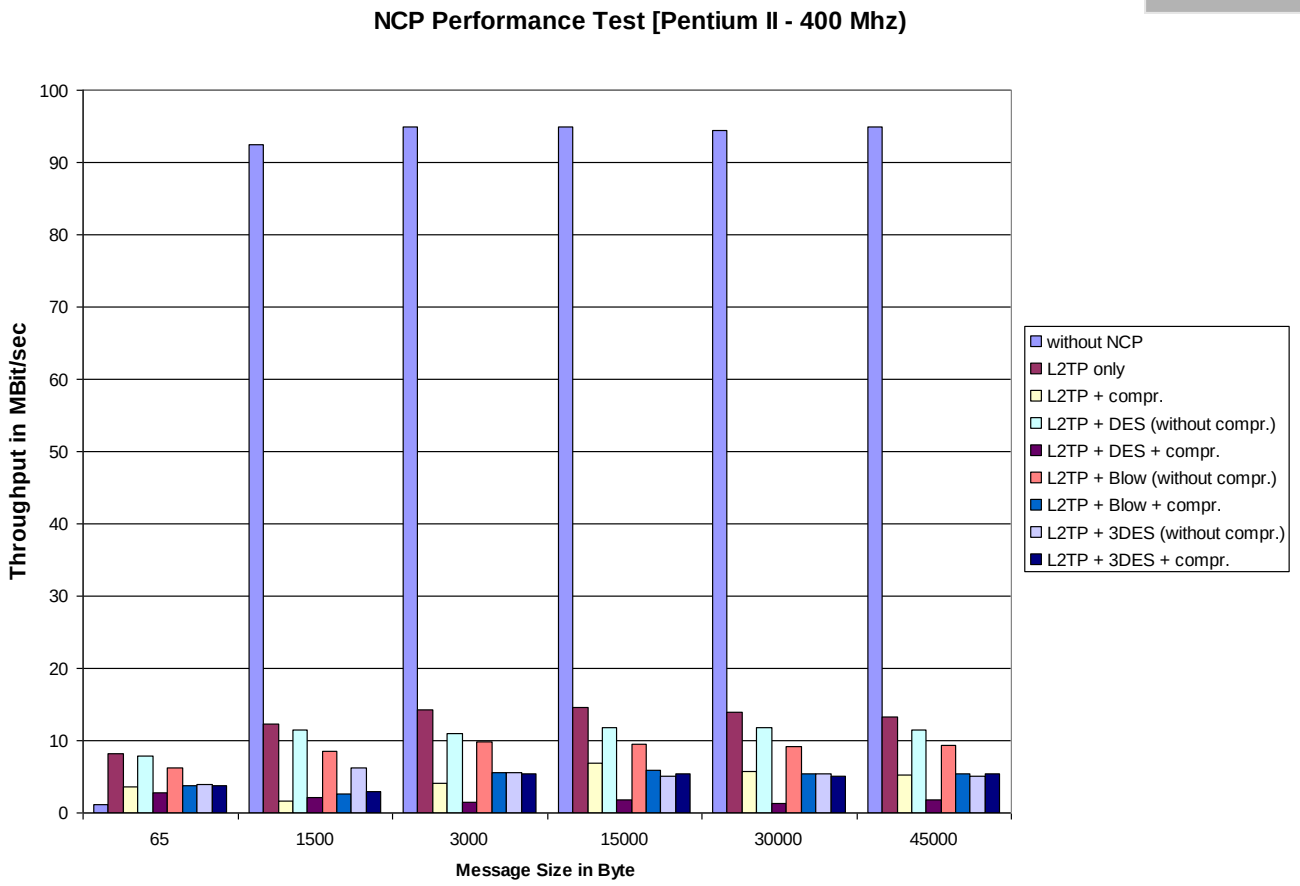
© DECOIT GmbH

Testparameter NCP

- **Variante A:** Ein Gateway-Eintrag wird lediglich beim physikalischen Adapter verwendet. Hierdurch werden nur die im LWS/Sec-Monitor angegebenen Netze über Tunnel erreicht.
- **Variante B:** Verwendet im Gegensatz zur Variante A einen Gateway-Eintrag lediglich beim virtuellen Adapter. Dies bewirkt, dass der gesamte Datenverkehr über den Tunnel stattfindet. Es wird jedoch ein Eintrag in der Routing-Tabelle benötigt, der für den erstmaligen Tunnelaufbau vom LWS/Sec-Client zum MPR/GA-Gateway verantwortlich ist.

© DECOIT GmbH

NCP



© DECOIT GmbH

Zusammenfassung

© DECOIT GmbH

Problemfelder

- Proprietäre Lösungen am Markt vorhanden
- IPsec ist nicht immer kompatibel durch Abweichungen
- Technische Abhängigkeiten durch den Provider
- Nicht alle Anwendungen arbeiten fehlerfrei
- Politische Hürden durch unterschiedliche Verschlüsselung
- Bandbreite/Performance kann über das Internet nicht garantiert werden
- Zusätzliche Rechenzeit für Ver- und Entschlüsselung
- VPN-Management sollte in Benutzerverwaltung integriert sein
- Accouting & Billing fehlt

© DECOIT GmbH

Vorteile von Extranets/VPNs

- Flexibilität und Schnelligkeit im Partnermanagement
- Optimierung der Geschäftsprozesse
- Garantierte Verfügbarkeit, Qualität, Geschwindigkeit und Sicherheit der verfügbaren Information
- Durchgängiger elektronischer Kreislauf
- Keine geografischen Einschränkungen
- Keine Einschränkung der Sicherheit oder Vertraulichkeit der Daten
- Keine Medienbrüche
- Ausweitung des Unternehmensnetzes auf die Integration externer oder geschlossener (definierbarer und gestuft authentisierter) Benutzergruppen
- Flexible Einbeziehung mobiler Mitarbeiter
- Kommunikationsengpässe verteilter Geschäftsprozesse wird gelöst
- Jedes Unternehmen kann von Extranets profitieren

© DECOIT GmbH

Kosten-/Nutzenanalyse

- Für jede VPN-/Extranet-Lösung muss eine Kosten-/Nutzenanalyse bezüglich der unterschiedlichen Realisierungsmöglichkeiten erfolgen
- Argumentation fällt dadurch gegenüber der Geschäftsleitung/Controlling wesentlich leichter
- Bei richtiger Dimensionierung lassen sich fast immer Kosten einsparen
- Weitere Parameter wie Verfügbarkeit, QoS/CoS, Management, Skalierbarkeit, Migrationsfähigkeit etc. müssen ebenfalls einbezogen werden

© DECOIT GmbH

Fazit

- Extranet- und VPN-Lösungen werden für jedes Unternehmen eine Rolle spielen
- Anforderungen sind mit denen von Standleitungen gleichzusetzen
- Mannigfaltige Hersteller-/Produktlösungen sind vorhanden
- IPsec schafft notwendige Interoperabilität zwischen den verschiedenen Lösungen
- Performance wird durch Verschlüsselung stark eingeschränkt (Software versus Hardware)
- Kosten-/Nutzenanalyse sollte gegenüber anderen Lösungen erfolgen
- Analyse der genutzten Applikationen erforderlich

© DECOIT GmbH

Buchtip zum Thema

Extranet - VPN-Technik zum Aufbau sicherer Unternehmensnetze

Addision-Wesley-Verlag; Pearson Education Deutschland GmbH; ISBN 3-8273-1674-X; München 2001

Autoren: Detken, Eren

detken@decoit.de

© DECOIT GmbH