VPN: SSL vs. IPSec

erfrakon - Erlewein, Frank, Konold & Partner
Martin Konold
Dr. Achim Frank

Präsentation auf dem

IT Security Forum
9. November 2005, Frankfurt

erfrakon

erfrakon
Erlewein, Frank, Konold & Partner

- Seit Januar 2002 als Partnerschaftsgesellschaft
- Drei Inhaber (ehemals SuSE Linux Solutions AG – Stuttgart)
  - Dipl.-Ing. Tassilo Erlewein (RZ Uni-Stuttgart)
  - Dipl.-Phys. Martin Konold (KDE)
  - Dr. rer. nat. Achim Frank (MPI)
- Kundenstruktur
  - Automotive Sector
  - Maschinenbau
  - Öffentliche Hand

Warum VPN?

- Anbindung Firmenteile

  technisch: koppeln von IP-Netzen (**LAN-Kopplung**)

- Anbindung von Außendienstmitarbeitern, Heimarbeitsplätzen und Wartungszugängen,

  technisch: anbinden eines (mobilen) Arbeitsplatzes an das Firmennetz (**Road Warrior**)

  Heute bestehen VPN Lösungen aus:
- IPsec
- SSL
- andere sichere Verfahren (SSH Port Forwarding)
- Andere unsichere/zweifelhafte Verfahren (MS PPTP, aber auch Open Source Verfahren)

VPN Technologien (1): IPSec 1

- IETF RFC 2401 „Sicherheitsarchitektur für IP“
- IETF RFC 2402 AH (IP Protokoll 51) – rein akademisch / keine Vertraulichkeit
- IETF RFC 2406 ESP (IP Protokoll 50) – Authentifizierung, Integrität und Vertraulichkeit
- IETF RFC 2408 ISAKMP (Internet Security Association and Key Management Protocol)
- IETF RFC 2409 IKE (Internet Key Exchange)
- Initialer Schlüsselaustausch
  - Manual keying
  - IKE (UDP Port 500 als Quell- und Zielport)
    Aggressive Mode: unsicher / Main Mode: sicher
  - Verbindungskontext -> Security Association (SA)
- Zwei unterschiedliche SAs möglich:
  - Transport mode (Point-to-Point)
  - Tunnel mode (Gateway-to-Gateway)

VPN Technologien (1): IPSec 2

- IPsec wurde für IPv6 entwickelt und auf IPv4 rückportiert
- Verbindungsaufbau
  - IKE (Quell- und Zielport 500 UDP)
  - NAT Traversal (Quellport beliebig, Zielport 4500 UDP)
- Authentifizierung
  - Ursprünglich nur PSK (Pre Shared Keys)
  - Heute: X.509v3 bevorzugt (Fragmentierungsproblem)
- Verschlüsselungsalgorithmen lt. RFC 2401:
  - DES in CBC mode
  - HMAC mit MD5 oder SHA-1 Hashes
  - NULL!
  - Nicht im ursprünglichen Standard: AES (schnell), 3DES (langsam),... !

VPN Technologien (2): Secure Socket Layer (SSL)

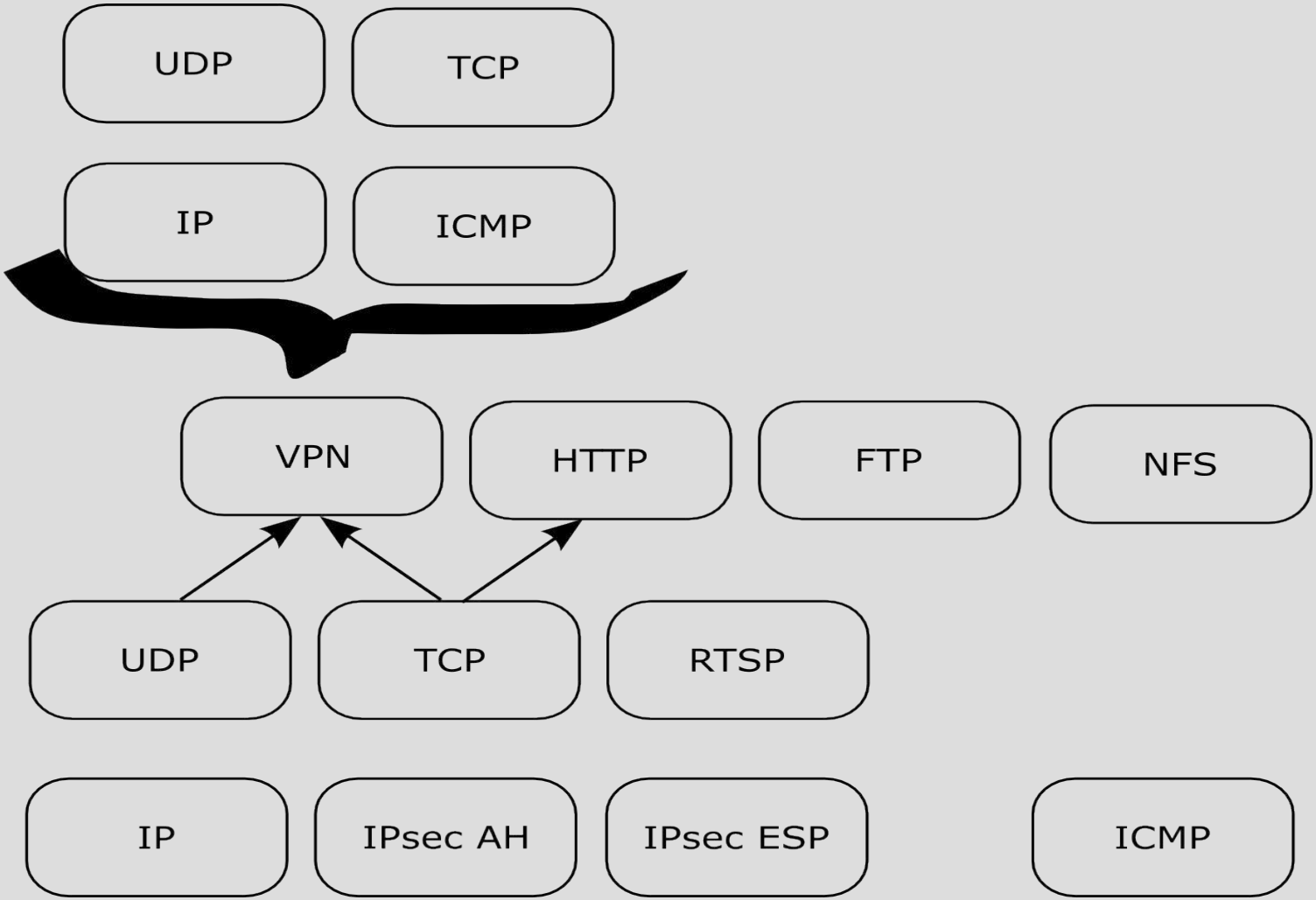
- Netscape (08/1994) SSL 1.0
- Netscape (12/1994) SSL 2.0
- Microsoft (11/1995) PCT 1.0
- Netscape (11/1995) SSL 3.0
- IETF RFC 2246 (01/1999) SSL 3.1 / TLS 1.0
- IETF RFC 2818 (05/2000) HTTP over TLS
  Ziel: Sichere Übertragung von HTTP Informationen

- Kryptographie analog zu IPSec: symmetrische, asymetrische Verschlüsselung, Hashfunktionen zur Integritätssicherung, x509 Zertifikate für Client und Server

- Implementierungen sind schwierig – immer wieder Sicherheitsprobleme (exploits)

- Mit dieser Technologie können VPN's gebaut werden – unterschiedliche VPN Implementierungen

Vergleich SSL vs. Ipsec 1



Vergleich SSL vs. Ipsec 2

	SSL	Ipsec
Memory	O	++
CPU	O	+
Bandbreite	+	++
Latenz	O	+
Vendor Support	+	++
Interoperabilität	O	-
NAT	++	-
LAN Kopplung	+	++
Road Warrior	++	-
Robustheit	+	++
Security	+	++

Was ist besser?

Es kommt auf die Details an...

Praxisbeispiel

Praxis: Mittelständler (Ausgangssituation)

- Intranet aus mehreren LANs
- Wartungszugänge (ISDN) z.B. f. Maschinen
- Außendienstler (ISDN) RAS
- Niederlassungen per ISDN Standleitung verbunden
- Niederlassungen breitbandig per Frame Relay Standleitungen (teils im Ausland)

Analyse des Bestands (1)

- Tragende Rolle spielt ISDN:
  - ist kein zeitgemäßer Zugang mehr – keine Verschlüsselung – unzureichende Authentifizierung
  - Technische Beschränkungen (128 kBit/s bei Kanalbündelung)
  - Angewiesen auf Carrier
  - Kosten/Nutzen Verhältnis sehr viel ungünstiger als bei „normalem“ Internetzugang

Analyse des Bestands (2)

- Standleitungen zur Koppelung bei größerer Bandbreite
  - Carrier managed equipment
  - Wenig Auswahl in Bezug auf Bandbreite
  - Teilweise kein Wettbewerb an bestimmten Standorten, d.h. hohe Preise

Alternative: VPN (1)

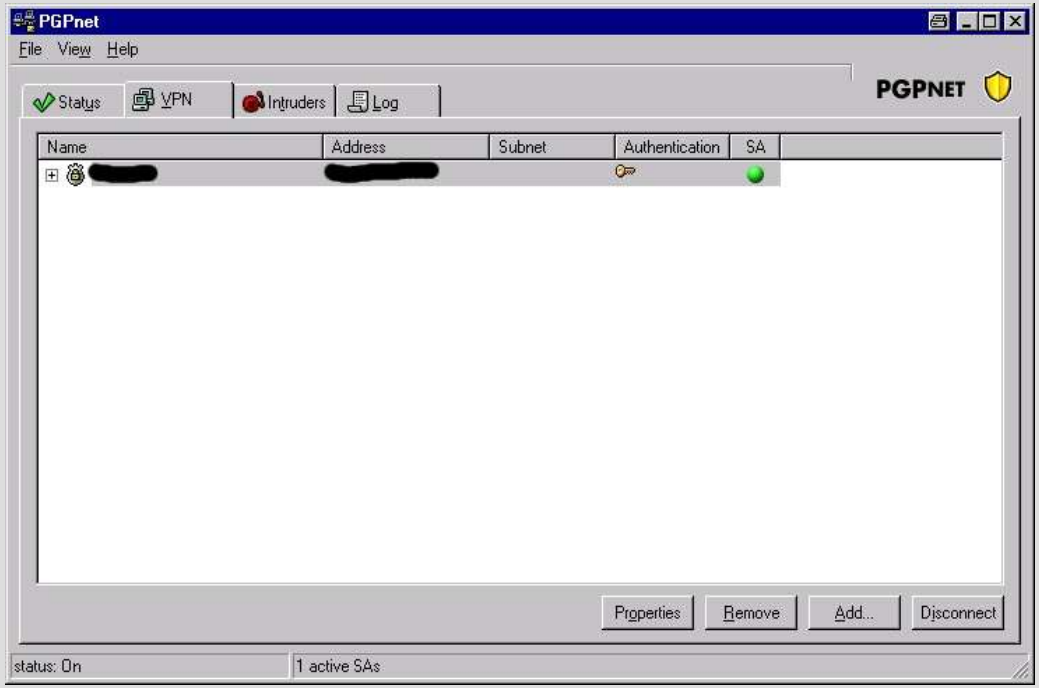
- Jeder Standort der vernetzt werden soll (Stammsitz, Niederlassungen, Außendienst MA, Wartung, ...) braucht nur noch einen Internetzugang
- Da vertrauliche Daten ausgetauscht werden ist Verschlüsselung und Integrität von höchster Wichtigkeit
- VPN's können direkt von Carriern gekauft werden
- VPN Funktionalitäten können in bestehende Firewalls eingekauft und eingebaut werden

Alternative: VPN (2)

- Spezielle VPN Hardware Lösungen sind verfügbar
- Wichtig: „Military Grade encryption“, Authentizität und Integrität
- Zu prüfen: Kryptographische Implementierung der Algorithmen – Open Source Lösungen!
- Administrierbarkeit des VPN's
- Kosten für Wartung

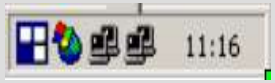
Praxis: Mittelständler (Entwicklung des VPN 1)

- VPN zwischen Standorten auf Basis von FreeSWAN (Linux IPSec) zwischen Gateways
- Mobiler Einsatz mit Windows Road Warriors unter PGP Net (2001)



Praxis: Mittelständler (Entwicklung des VPN 2)

- Integration von Wartungszugängen über eingebaute IPSec Funktionalität diverser Router
- Mobiler Zugang mit Windows 2000 bzw. XP nativem IPSec leider nicht benutzbar...
- Road Warrior unter SSH Sentinel ab 2003



- Bei IPSec Clients immer problematisch in welcher Reihenfolge Software installiert wird – Eingriff der IPSec Software ins Betriebssystem...

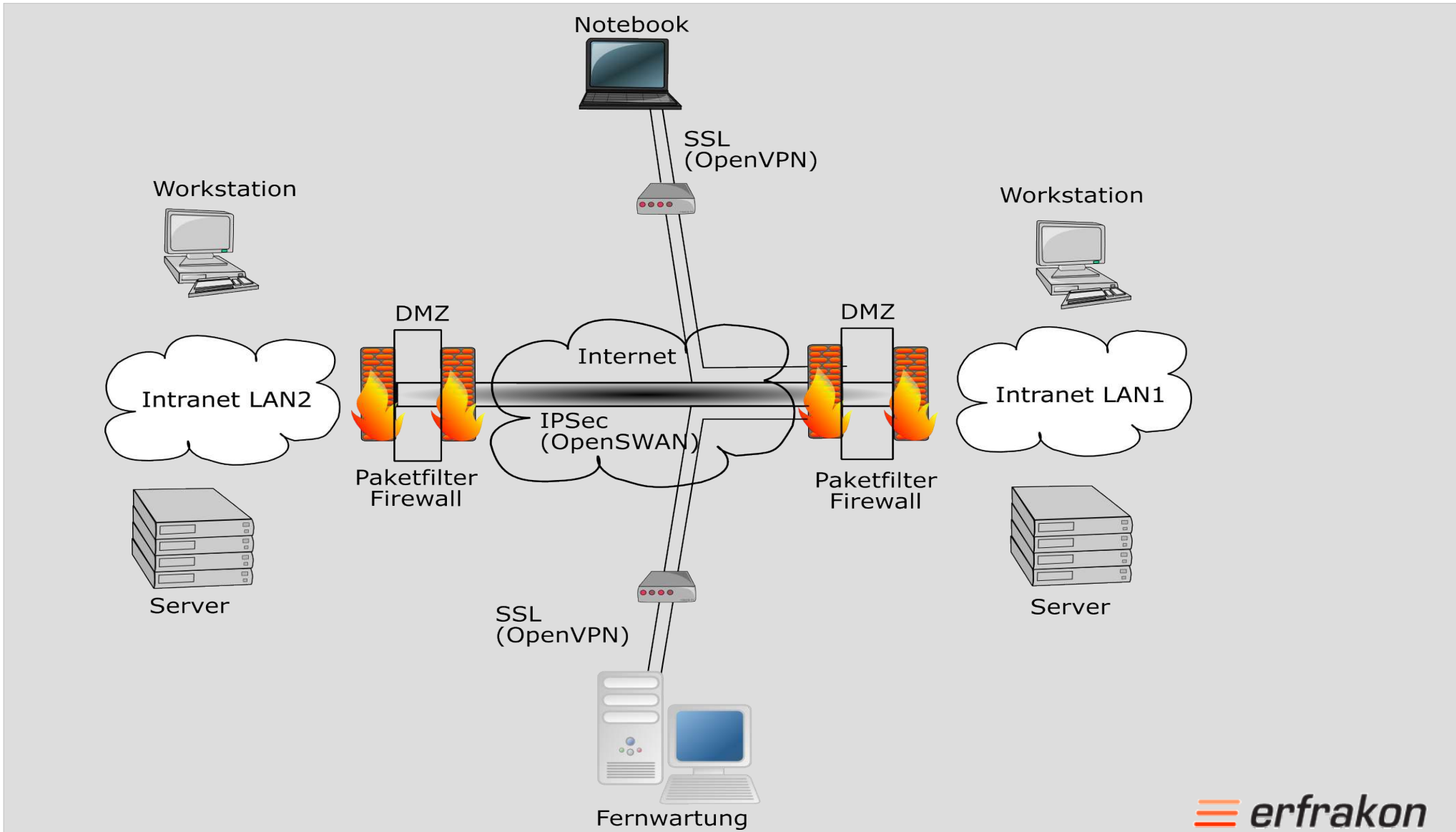
Praxis: Mittelständler (Entwicklung des VPN 3)

Heute:

- FreeSWAN durch OpenSWAN auf Linux Gateway ersetzt
- IPSec zwischen Standorten hat sich bewährt
- IPSec für Road Warriors und teilweise bei Wartungszugängen ersetzt durch OpenVPN (SSL)

- Probleme bei der Road Warrior Einrichtung mit Einsatz von OpenVPN deutlich zurückgegangen: es wird ein virtuelles Ethernet Interface benutzt – keine Konflikte mit Windows System

Typisches Netzwerk



erfrakon

Zukünftige Entwicklungen

- Sicherheitsproblematik: das gesamte VPN nur so sicher wie das schwächste Glied, d.h. ein Windows Notebook...
- Immer mehr Heimarbeitsplätze werden geschaffen – wie anbinden?
- Durch Heimarbeits-PC's darf keine Gefährdung des Unternehmens LAN's möglich sein
- Datendiebstahl aus Firmennetz?

Zugänge auf Basis von Terminalserver Lösungen:
NX als Open Source Lösung

Danke für Ihre Aufmerksamkeit

Noch Fragen ?

Sprechen Sie uns an!

erfrakon - Erlewein, Frank, Konold & Partner
Martin Konold
Dr. Achim Frank