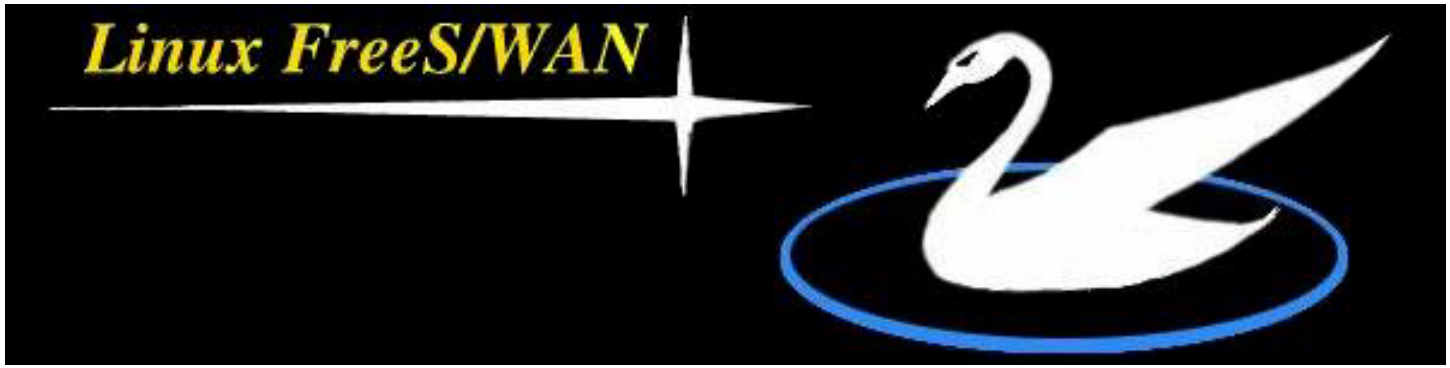


VPN/IPsec

Grundlagen und praktische Erfahrungen in der Kopplung von Linux (FreeS/WAN) und Windows 2000

Holm Sieber <sieber@prudsys.com>

Alexander Schreiber <als@thangorodrim.de>

Begriffsdefinitionen

VPN: virtuelle private Netze

Punkt-zu-Punkt-Verbindung über im Allgemeinen TCP/IP-Netzen

IPsec: gesicherte Verbindung in unsicheren Netzen, das heißt:

- Authentifizierung und/oder
- Verschlüsselung

Andere VPN-Software

- **CIPE:**
  http://sites.inka.de/sites/bigred/devel/cipe.html
  - Linux
  - Windows
- **VTUN:**
  http://vtun.sourceforge.net/
  - Linux
  - Solaris
  - alle BSD-Varianten

Verschlüsselungsverfahren

- symmetrische Verfahren:
  - 3DES (Triple DES)
  - Blowfish (nicht im FreeS/WAN genutzt)
  - IDEA (nicht im FreeS/WAN genutzt)
- asymmetrische Verfahren:
  - RSA (**R**ivest **S**hamir **A**dleman public key algorithm)
  - Diffie-Hellman (DH) key exchange protocol

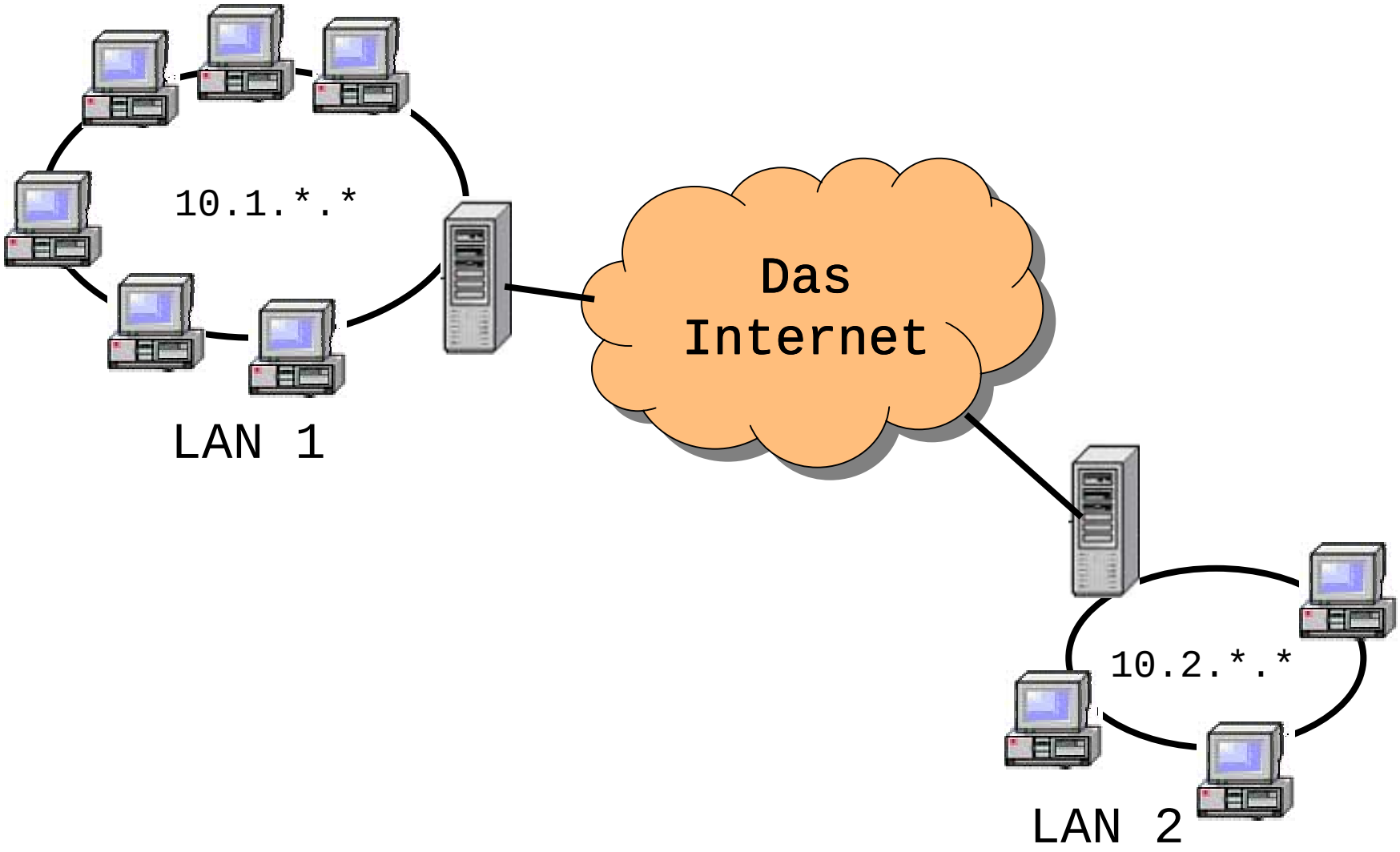
Standards zu IPsec

- RFC 2401 (IPsec)
- RFC 2409 (IKE, Internet Key Exchange)
- RFC 2408 (ISAKMP, Security Association and Key Management Protocol)
- RFC 2412 (Oakley Key Determination Protocol)
- ... und einige weitere RFC

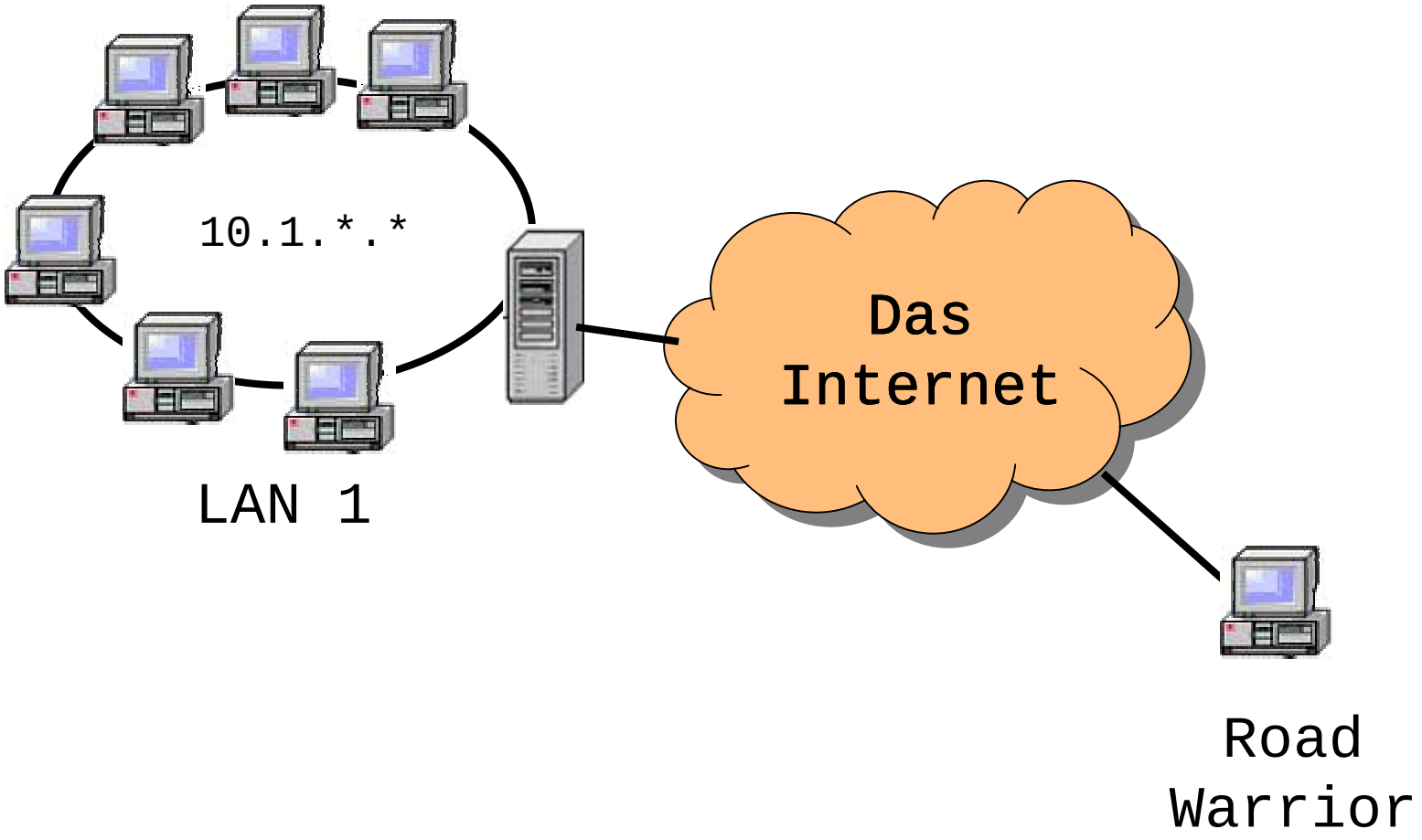
Kompatibilitäten

- FreeS/WAN
- Windows 2000 und Windows XP
- Hardware von Cisco, Nortel und anderen Anbietern
- Client-Software SSH Sentinel oder PGPNet

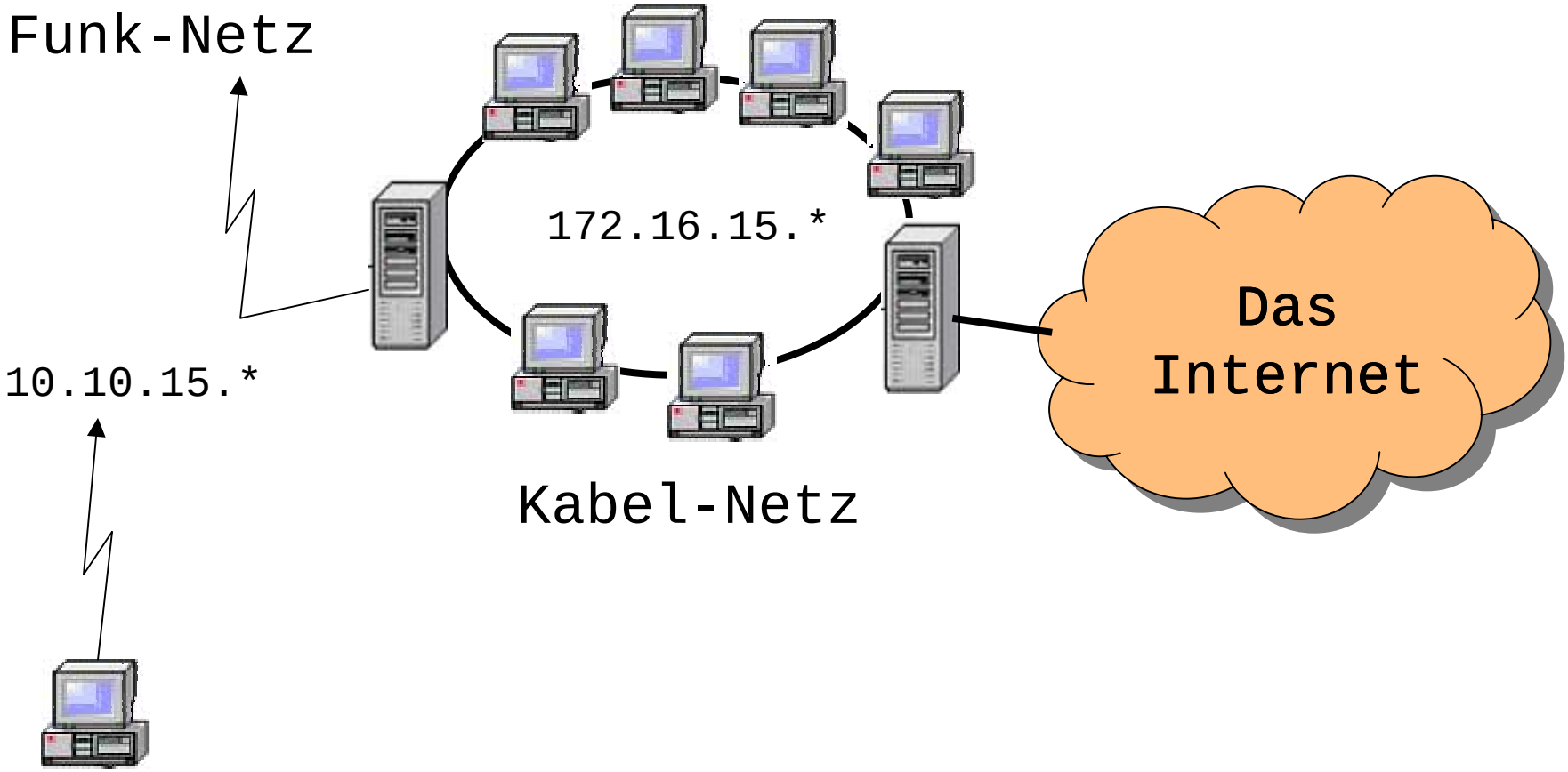
Beispiel 1: LAN-Kopplung



Beispiel 2: Road Warrior



Beispiel 3: Sicheres Funk-LAN



Installation 1: Key-Generierung

Für die Authorisierung werden X.509 Zertifikate benötigt, die mit openssl generiert werden können:

- Root CA
- FreeS/WAN Gateway Zertifikat
- Road Warrior Zertifikat

Beschreibungen:

- c‘t 2002, Heft 5, Seite 220 ff.
- http://vpn.ebootis.de/cert.htm
- http://www.natecarlson.com/include/showpage.php?cat=linux&page=ipsec-x509

Installation 2: FreeS/WAN-Server

- Kernel 2.4 incl. X.509 Patch (evtl. auch schon im FreeS/WAN-Paket eingespielt)
- FreeS/WAN installieren (im Allgemeinen als Paket fertig)
- /etc/ipsec.conf anpassen
- Keys installieren:
  - RSA-Keys in /etc/ipsec.secrets
  - X.509 Keys unter /etc/ipsec.d/
- Routing konfigurieren!

Installation 3: Windows 2000

- Benötigt:
  - ipsecpol.exe von Microsoft (siehe google)
  - IPsec-Tool von Marcus Müller (http://vpn.ebootis.de/package.zip)
- Keys über mmc installieren
- ipsec.conf anpassen

Links

1 http://vpn.ebootis.de/

2 http://www.freeswan.org/

3 http://sunsite.dk/vpnd/

4 http://stunnel.mirt.net/

5 http://cag.lcs.mit.edu/~cananian/Projects/PPTP/

6 http://www.hsc.fr/ressources/ipsec/ipsec2001/

7 http://www.hsc.fr/ipsec/ipsec2001/

8 http://www.linuxdoc.org/HOWTO/VPN-Masquerade-HOWTO.html

9 http://www.strongsec.com/freeswan

10 http://www.openssl.org