VPN Zugang

PPTP-VPN-Zugang mit OpenSource-Mitteln

Oktober 2004, Best-Practice-Papier zum IT-Sicherheitskonzept der FH Gelsenkirchen.

1 Ziele

Mit Hilfe von frei verfügbarer OpenSource-Software soll ein VPN-Zugang ermöglicht werden, der es erlaubt über das Internet Dienste und Daten im internen Netzwerk nutzen bzw. erreichen zu können.

- Einfacher Client-Zugang (wenn möglich ohne Zusatzprogramme, sondern nur mit Programmen, die das Betriebssystem mitbringt)
- Plattformübergreifend nutzbar
- Integration in bestehende Authentikationsstruktur (siehe Best-Practice Papier zum Thema „Zentrale Benutzerauthentikation")

2 Voraussetzungen

- Hardware:
  - 1 Linux PC mit Kernel >= 2.4, Empfehlung: Kernel: xxx
  - Schnittstellen zu den verfügbaren Netzwerken
- Internetzugang
- Intranetzugang
- PPP > Version 2.4.2 (MPPE Unterstützung)

3 Struktur

3.1 IT-Struktur

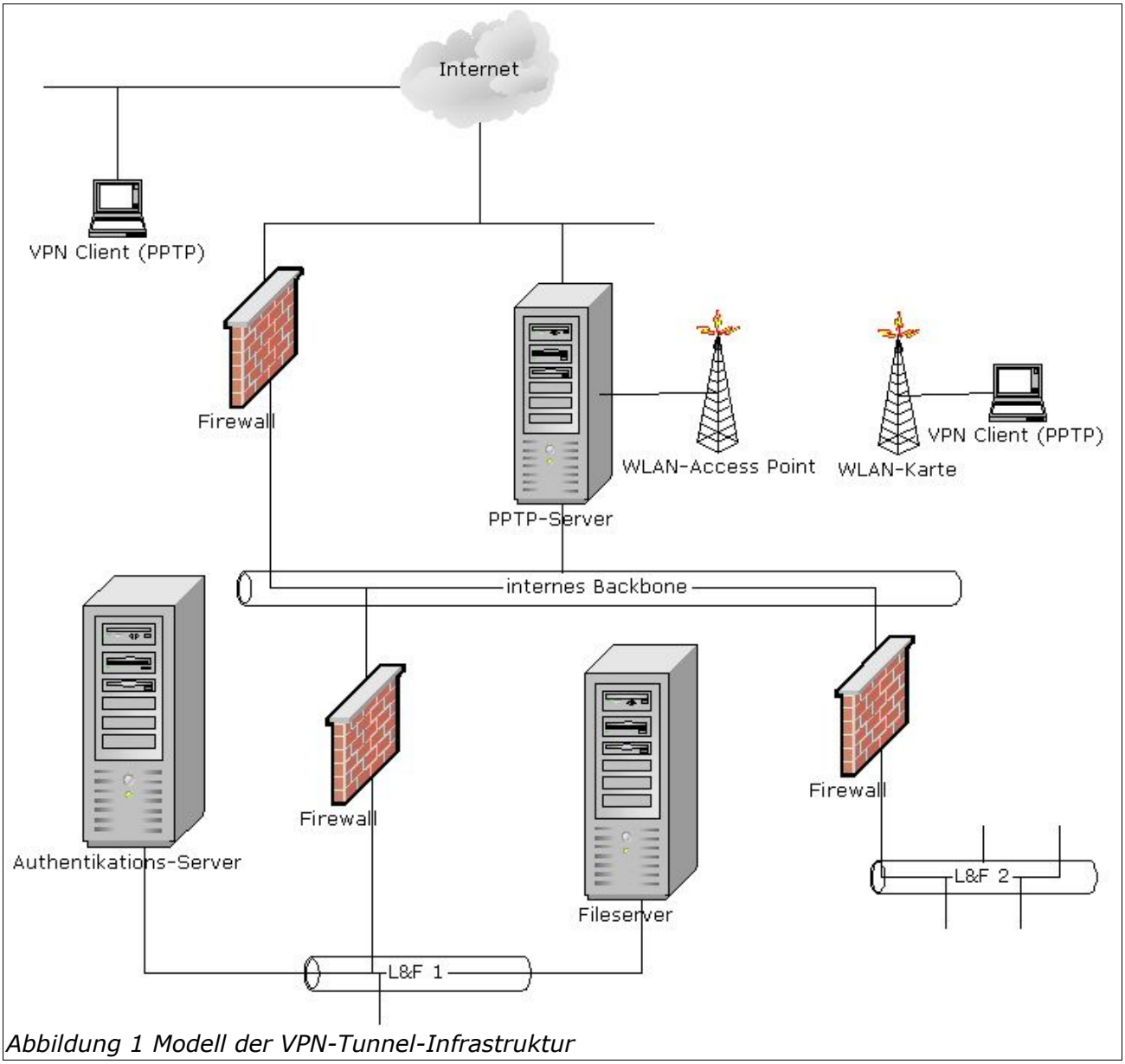

Abbildung 1 Modell der VPN-Tunnel-Infrastruktur

Das Diagramm zeigt die IT-Struktur mit dem PPTP-Server als Kernstück. Dieser Server muss aus dem Internet erreichbar sein und ist ein Endpunkt des VPN-Tunnels.

Zur Authentikation nutzt der pppd standardmäßig eine Datei, er kann allerdings auch so konfiguriert werden, dass er einen Authentikations-Server zur Authentikation nutzt (z.B. LDAP).

3.2 Zugangskontrolle

Der PPTP-Server erfordert zunächst eine gültige Authentikation, um in das interne Backbone zu gelangen. Von dort aus sind dann jedoch noch nicht unmittelbar alle Dienste erreichbar.

Um dann Dienste aus eventuell unterschiedlichen Lehr- und Forschungsbereichen nutzen zu können, muss sich der VPN Client gegenüber den Firewalls der entsprechenden Lehr- und Forschungsbereiche authentifizieren. Dies kann beispielsweise über das Mounten einer entfernten, passwortgeschützten Samba-Share erfolgen (im Diagramm L&F 1).

Sobald die Share gemountet wird, schaltet die L&F 1-Firewall den Zugriff auf das interne Netz des L&F 1 frei.

Routing aus dem VPN-Tunnel ins Internet wird unterbunden.

3.3 WLAN

Der VPN-Zugang kann unverändert mit einer weiteren Schnittstelle zum WLAN zur Absicherung eines drahtlosen Netzwerks genutzt werden.

Durch ein zusätzliches Attribut in der LDAP Authentikation kann auch getrennt der Zugriff auf WLAN/VPN aus dem Internet kontrolliert werden.

4 Installation/Einrichtung

4.1 Server

Die meisten aktuellen Linux Distributionen bringen bereits ppp und pptp Pakete mit. Die Standardpakete erlauben den Betrieb des PPTP-Servers allerdings nur mit dateibasierter Authentikation.

Der PPP-Daemon pppd muss, falls die Authentikation nicht über eine Datei, sondern über LDAP erfolgen soll gepatcht und neu kompiliert werden.

4.2 Clients

Windows

Windows bringt seit Version 9x und NT4 alles Notwendige mit, um den PPTP Zugang nutzen zu können. Microsoft hat zwischenzeitlich ein Update verfügbar gemacht, mit dem unter Windows 9x/ME auch 128-Bit-Verschlüsselung möglich ist. Die neueren Betriebssysteme bringen dieses Feature bereits mit.

Für Anleitungen zur Einrichtung der Clients siehe Dokumentation auf www.poptop.org .

Linux

Siehe Anhang A.

4.3 Quellen und ergänzende Informationen

- www.poptop.org, POPTOP Projekt, VPN via PPTP