Löst IPv6 die VPNs ab?

Lutz Donnerhacke

IKS GmbH

http://[2001:4bd8::1]

Das Internet – unendliche Weiten

- Wir schreiben das Jahr 1982:
  - Jeder, der will, bekommt IP Adressen
  - Angeschlossene Systeme kommunizieren direkt
  - Stürmische Protokollentwicklung nach dem Motto „Sprich Freund und tritt ein“
- Aufgabe: Kampf gegen die übermächtige OSI

Das Internet – endliche Weiten

- Wir schreiben das Jahr 1996:
  - Adressknappheit droht
  - Beginn der Entwicklung an IPv6, bis dahin:
  - Effizientere Nutzung durch „Subnetting“
  - Erfindung des „Intranets“ mit privaten Adressen
  - Entwicklung von Hilfskonstrukten wie NAT & Proxy
- Aufgabe: Zugriff auf die Intranets ermöglichen

Das Internet – kommerzielle Inseln

- Wir schreiben das Jahr 2010:
  - Dynamische und private IP Adressen dominieren
  - Betriebsmodell: Kommerz bedient Kunden
  - Zugriff auf Ressourcen problematisch
  - Nur Overlaynetze gestatten Direktkommunikation
  - Mehrfach-NAT, Überfilterung vs. Tunneltechniken
  - Man spricht nicht miteinander, man bekämpft sich
- Entscheidung: Kommerz- oder Internet

Das Internet – unendliche Weiten

- Wir schreiben das Jahr 2022:
  - IPv6 ist weltweit das primäre Protokoll
  - Direktzugriff auf die beteiligten Systeme möglich
  - Viele mobilen Geräte tauschen Infohäppchen aus
  - Zentrale Informationsdrehscheiben sind pleite
  - Politik begreift ungefilterten Informationszugang als Grundpfeiler einer freien Gesellschaft
- Problem: Es droht Adressknappheit

IPv6 – Überblick

- **Direkte** Adressierbarkeit **aller** Geräte
- IPv6 vergrößert den Adressbereich
  - Genug „Platz“ für alle Anwendungen
  - Andere Adressen: „Hexzahlen und Doppelpunkte“
  - Endanwender erhalten 256 bis 65536 offizielle Netze
  - lokal/öffentlich, fest/privat, uni- ,multi-, anycast
- Mehrere Adressen pro Interface Pflicht
  - Autoconfig, Parallelbetrieb : Renumber, Multihoming
  - Voraussetzung für Mobilität

VPN – Lichtblick im Mangel

- Mobiler Zugriff auf private Netze
  - bedarfsgetriggerter Tunnel
  - Mobiles Gerät wird virtuell ins Netz eingeblendet
  - Zugriff über das böse Internet mit Kryptographie
- Klassischer Ansatz
  - Nutzer legt fest, wann VPN aktiv ist
  - Anschluss wie an einem langen „Kabel“
  - Entweder „im VPN“ oder „im Internet“

VPN – Erweiterungen

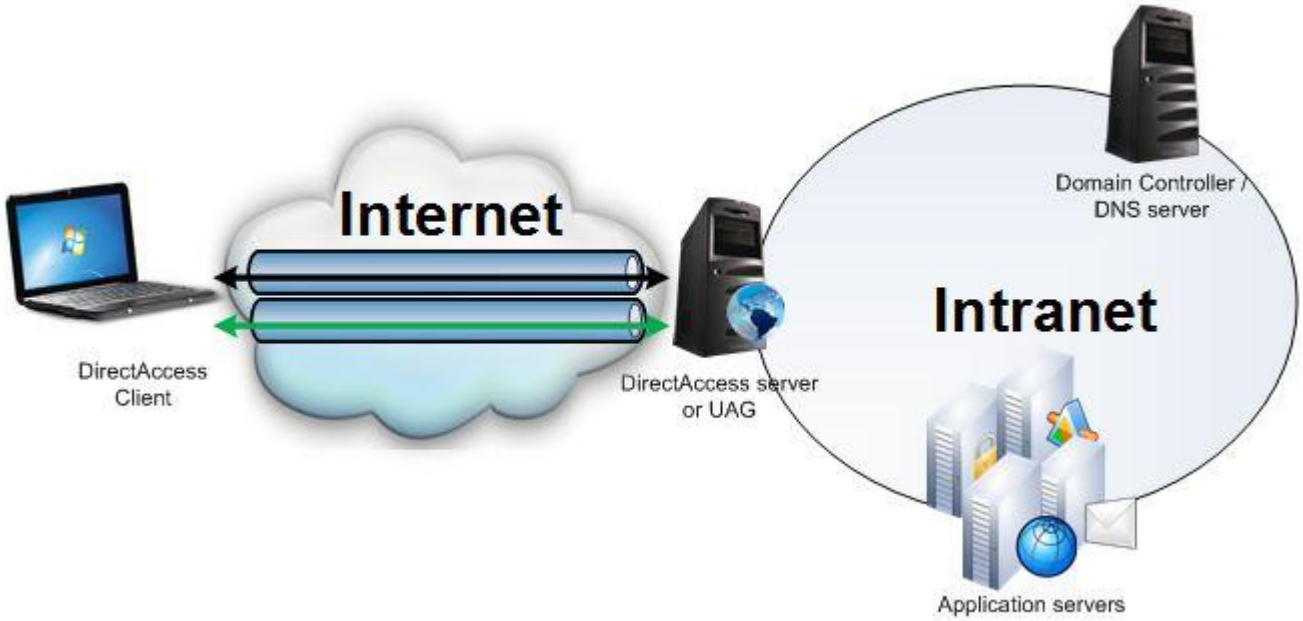
- Split-Tunnel für parallelen Zugriff
- NAT-Traversal für Zugriff aus privaten Netzen
- Dynamische Netzwerkkonfiguration
- VPN-Start vor Nutzer-Anmeldung
- Überprüfung des Client-Sicherheitsstatus
- Softwareverteilung via VPN
- Multiple Authentisierung (Computer, Nutzer)

Microsoft – DirectAccess

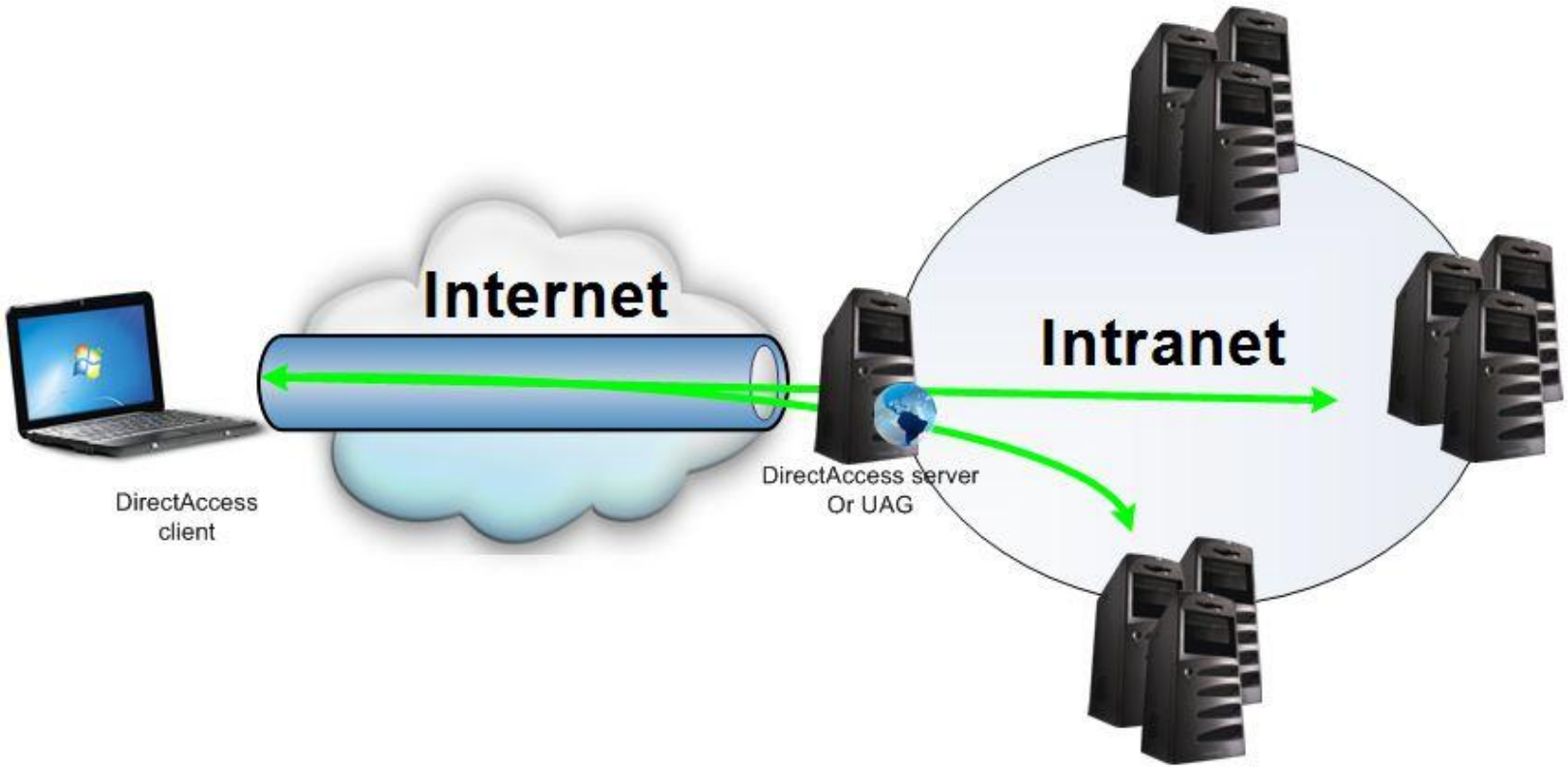
- Automatisiertes VPN
  - Ermittlung des Standorts (lokal oder remote)
  - IPSec Tunnel zwischen Computer und DA-Server für „lokalen“ Dauerzugriff auf den Rechner
  - IPSec Tunnel mit Nutzeranmeldung für Apps
  - Split-Tunnel dank DNS-Regeln
  - IPv6 statt IPv4 Adresspools und NAT
  - Automatische Tunnel und NAT bei Bedarf Teredo, 6to4, NAT64, IP-HTTPS

http://technet.microsoft.com/en-us/network/dd420463.aspx

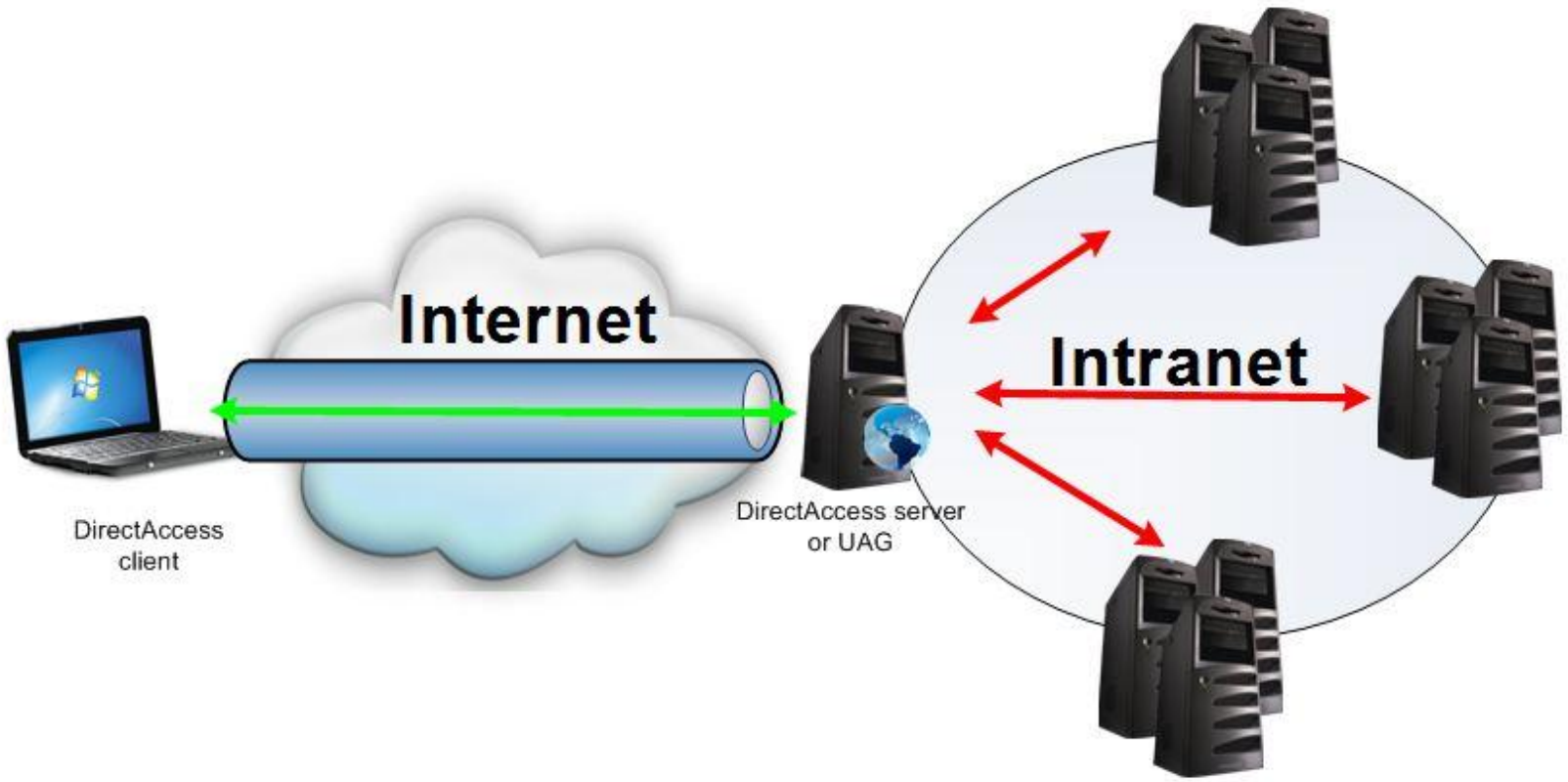
Microsoft – DirectAccess



Microsoft – DirectAccess



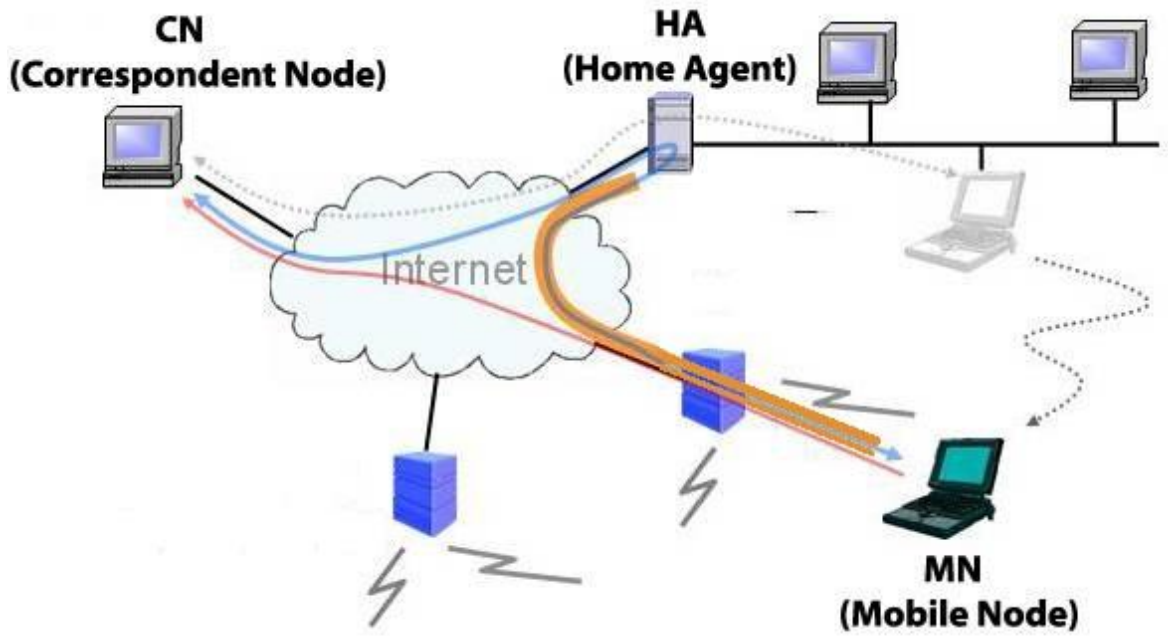
Microsoft – DirectAccess



Mobile IPv6 – unterwegs daheim

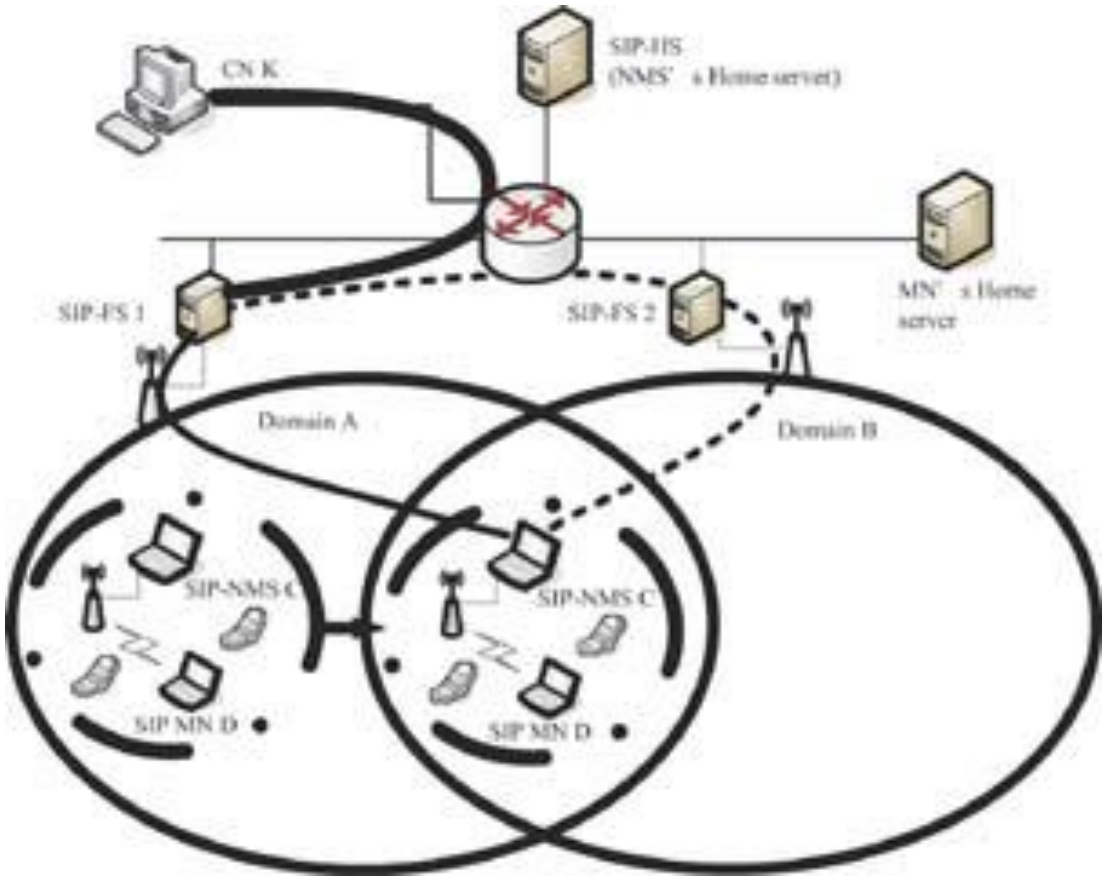
- Sicherstellen der Erreichbarkeit
  - Gerät hat viele IPv6 Adressen: Home, Care of, …
  - IP-Proxy im Heimnetz: Home Agent
    - Wenn HA direkt erreichbar, dann ist er im Heimnetz
    - Sonst sendet Client eine Bindungsanforderung (CoA)
  - Anfragen relayed der HA an den Client
    - Client sendet dem Anfrager eine Bindungsanforderung
    - Client redet mit Anfrager anschließend direkt
  - Fallback auf klassischen VPN Pfad

Mobile IPv6 – unterwegs daheim



NEtwork MObility: Mobile Router, der ganze Netze mitnimmt.

Mobile IPv6 – unterwegs daheim



Beim Roaming zu einem neuen Netz werden zwei Verbindungen gleichzeitig aufgebaut werden, auf denen die Pakete doppelt ankommen. So bricht eine bestehende Verbindung nicht ab.

Techniken im Vergleich

Anforderung	IPv6	VPN	DirectAccess	Mobile IPv6
Zugriff Internet	Ja	Split-Tunnel	Ja	Ja
Zugriff Intranet	Firewall	Ja	Ja	Ja
Feste Client IP	Nein	Im LAN	Im LAN	Ja
Nutzer bekannt	Nein	Ja	Ja	Nein
Automatisch an	Ja	Nein	Ja	Ja
Effizienter Datenfluss	Ja	Nein	Nein	Ja
Unterbrechungsfrei	Nein	Nein	Nein	Ja
Moderner Server	Ja	Nein	Ja	Ja
Legacy Server	Nein	Ja	NAT64	Nein
Moderner Client	Ja	Nein	Ja	Ja
Public Legacy Client	6to4	Ja	6to4	6to4
Private Legacy Client	Teredo	NAT-Traversal	Teredo	Teredo

Mobile IPv6 – Testen und Probieren

- Workshop „Mobile IPv6 in der Praxis“
- Frankfurt/Main, 20. und 21. Mai 2010

- http://www.ipv6-kongress.de/

Fragen?

Lutz Donnerhacke

dig NAPTR 1.6.5.3.7.5.1.4.6.3.9.4.e164.arpa. +dnssec

OpenPGP: DB089309 lutz@iks-jena.de
1C 1C 63 11 EF 09 D8 19 E0 29 65 BE BF B6 C9 CB