Windows 7

Remote Access mit IPv6

Community Treffen Network & Security
14. April 2010

Epp Stefan

Agenda

- Aufgabenstellung
- Transition Technologies
- Kurze Demo
- Name Resolution Policy Table
- NAT64 & DNS64
- Weitere Schritte

maxon motor ag

- IT Infrastruktur
  - Hauptstandort in Sachseln
  - 3 Produktionsstandorte
  - 14 Vertriebsgesellschaften
  - 1400 Clients

Aufgabenstellung

- Windows 7 Teilprojekt „Security“
- Proof of Concept für Remote Access
  - Microsoft DirectAccess anstelle der bestehenden Cisco Client VPN Infrastruktur
- Anforderungskatalog
  - Einhaltung Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit)
  - Unterstützung maxon Standardapplikationen
  - Benutzerfreundlichkeit und einfache Administration
  - Kosten

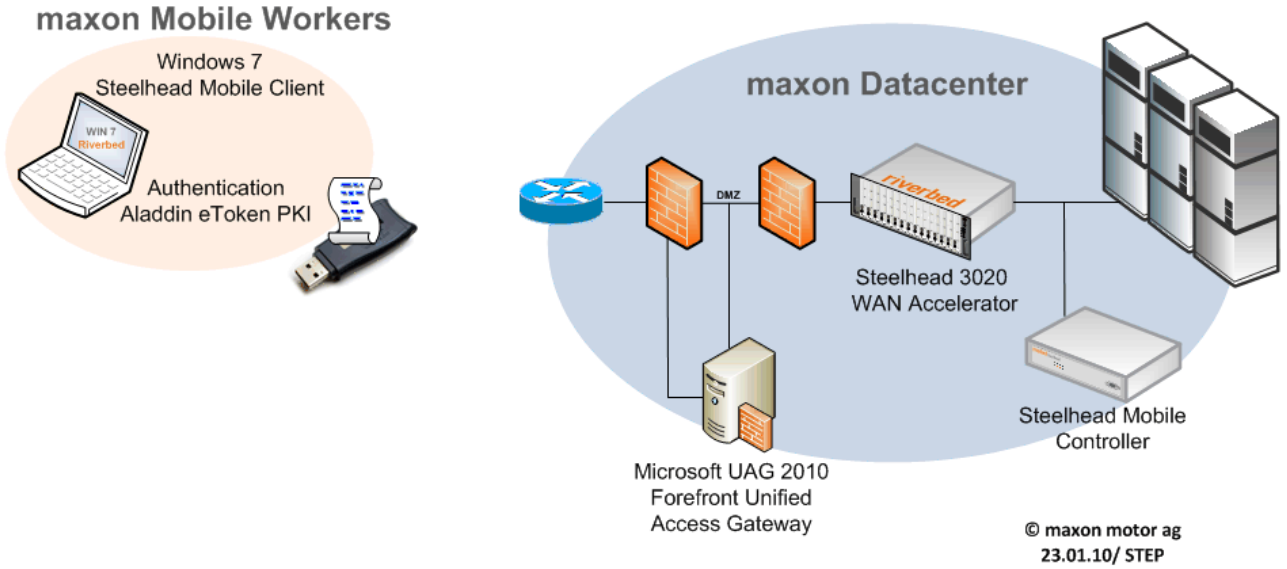
Was ist DirectAccess?

- Mit Windows 7 und Server 2008 R2 bietet Microsoft eine völlig neue Technologie im Bereich Remote Access an. Das Notebook benötigt nur noch eine Internetverbindung und schon kann der Benutzer auf firmeninterne Ressourcen zugreifen als würde er im Büro arbeiten.

- Innerhalb des IPsec Tunnels wird nur über IPv6 kommuniziert.

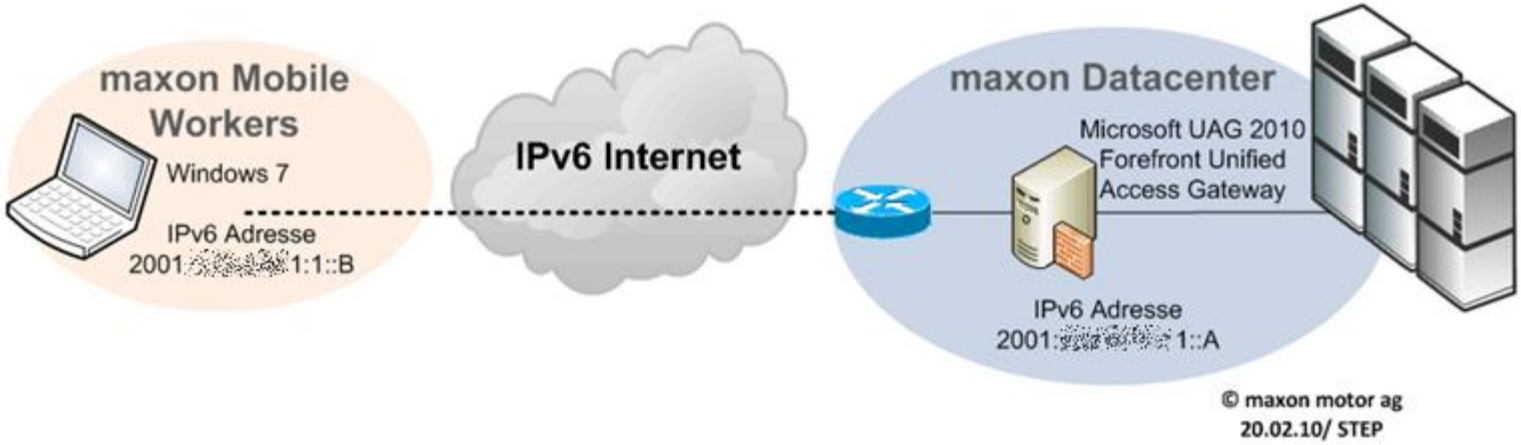
Aufbau Testumgebung

- Forefront Unified Access Gateway 2010
  - Forefront Threat Management Gateway (TMG) Nachfolgeprodukt von ISA



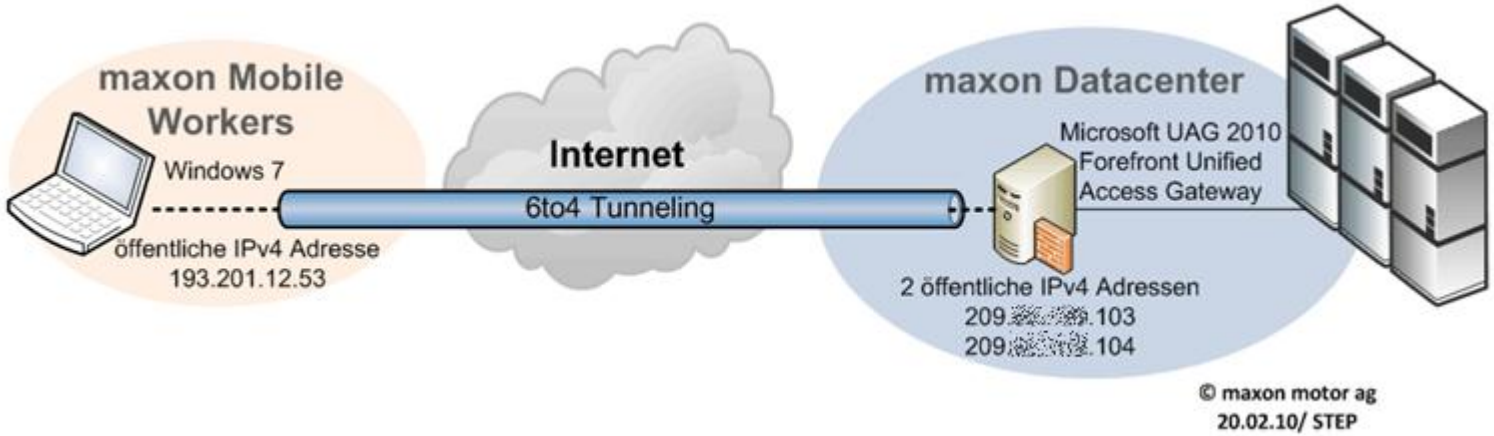
Transition Technologies

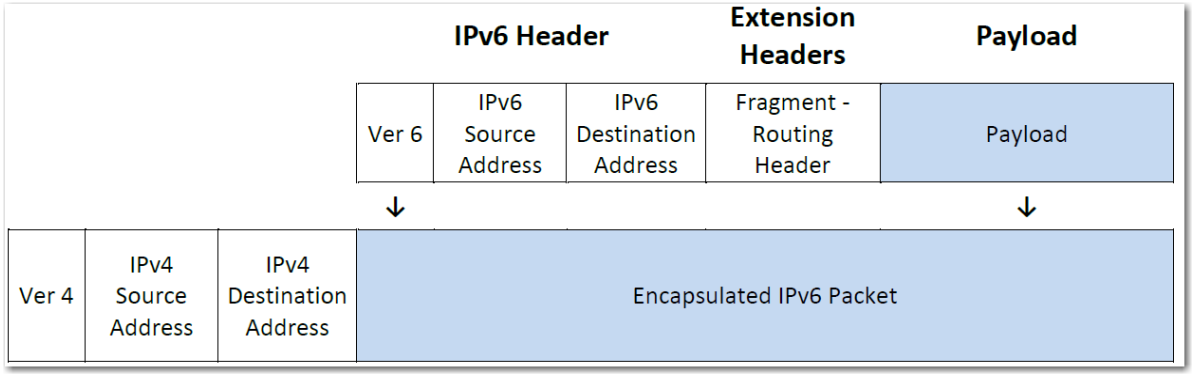
- Native IPv6
  - IP Protokoll 50
  - ICMPv6
  - UDP 500
  - Ideale Voraussetzung aber selten anzutreffen



Transition Technologies

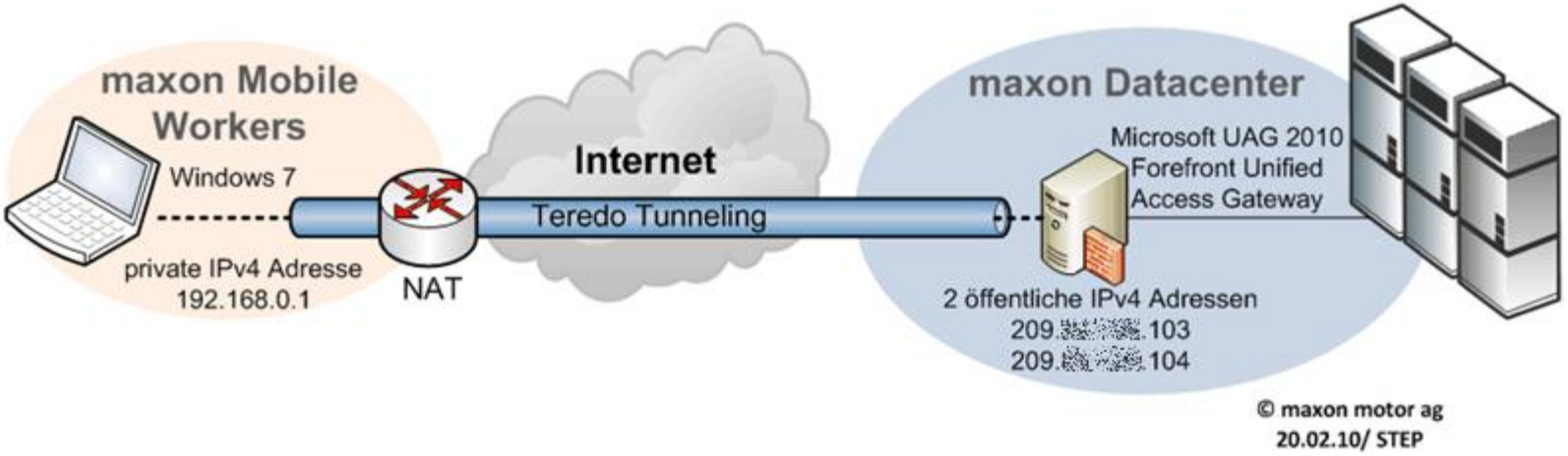
- 6to4 Tunneling
  - IP Protokoll 41





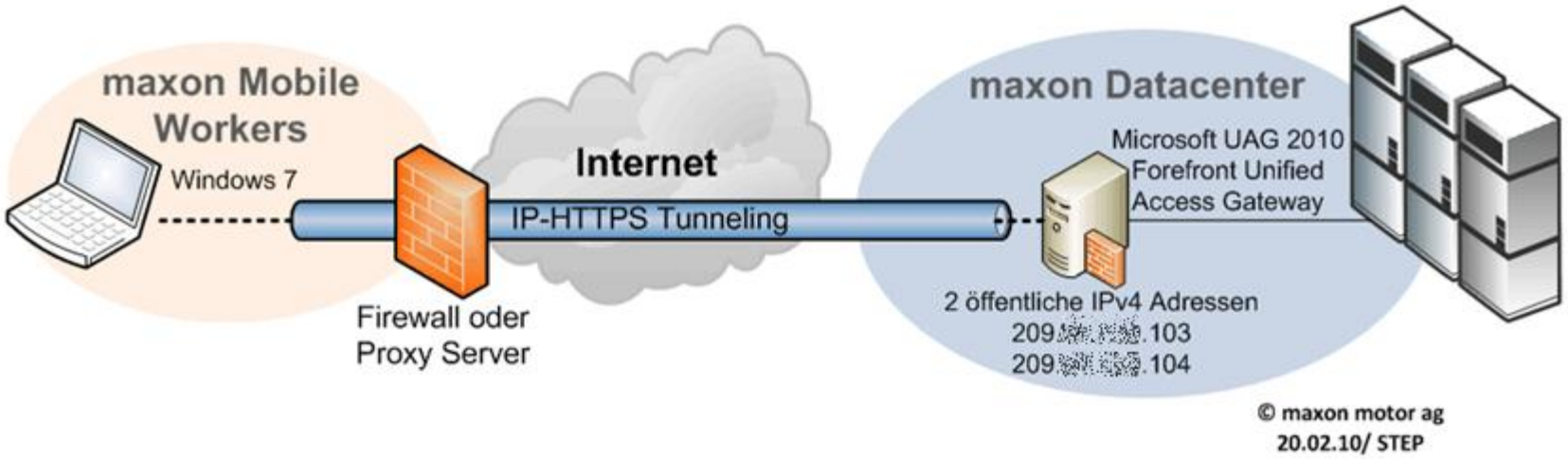
Transition Technologies

- Teredo Tunneling
  - UDP Port 3544 (aus Sicherheitsgründen oft gesperrt)
  - 2 öffentliche IPv4 Adressen wegen unterschiedlichen NAT Methoden
  - „Full Cone“ NAT und „Restricted Cone“ NAT



Transition Technologies

- IP-HTTPS Tunneling
  - TCP Port 443
  - Keine Unterstützung für Web Proxy mit Authentifizierung



DirectAccess Feature

- Name Resolution Policy Table (NRPT)
  - Zuweisung von internen und externen DNS Server
  - Bestimmen von firmenintern oder externen Netzwerken
  - shop.maxonmotor.com, hochverfügbarer HTTPS URL mit öffentlichem Zertifikat
  - Splitting Tunneling
  - Command „netsh namespace show policy“
- Authentifizierung
  - Benutzernamen und Kennwort (Windows Login)
  - Zweistufige Authentifizierung mit Smartcards
  - Computer muss Domain Member sein
  - NAP ist empfehlenswert

NAT64 & DNS64

- NAT64
  - Übersetzung von IPv6 zu IPv4
  - Nachfolge von NAT-PT
  - Draft IETF (Internet Engineering Task Force)
- DNS64
  - Übersetzung von „AAAA-Records“ zu „A-Records“
  - Draft IETF

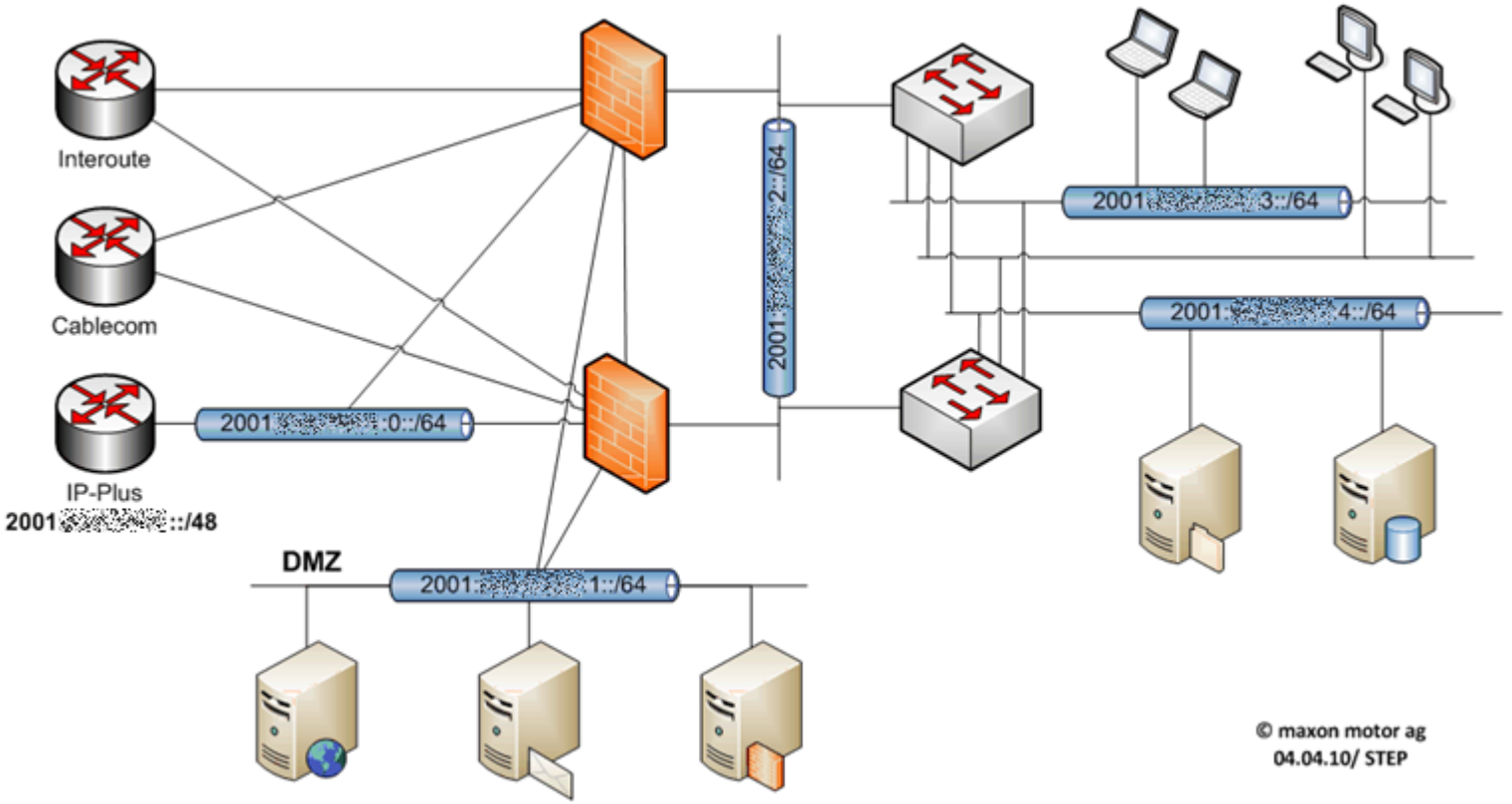
IPv6 Adresse	2002	d4[illegible]	[illegible]3d	8001	leer	ac[illegible]	102
Binär		11010100 [illegible]	[illegible] 11101	10000000 1		10101100 [illegible]	1 10
Dezimal		212 [illegible]	[illegible] 61	128 1		172 [illegible]	1 2
	Transition	externe DirectAccess IP Adresse		Transition		interne DNS IP Adresse	

Microsoft DirectAccess bei maxon motor ag

- Negative Aspekte
  - Keine Riverbed Unterstützung
  - Komplexität, der Projektaufwand ist schwierig abzuschätzen
  - Probleme mit OCS, Citrix und CA
  - Kein Provider Redundanz möglich
- Positive Aspekte
  - Noch nie da gewesene Benutzerfreundlichkeit
  - Für einen Zugriff ins Firmennetzwerk wird lediglich eine Internetverbindung benötigt
  - Auto-Reconnect bei Unterbruch
  - Einfaches Ausrollen über die GPO
  - Zum Verwalten der Clients muss der Benutzer nicht angemeldet sein

Weitere Schritte

- IPv6 wird weiter vorangetrieben
- DirectAccessRollout für IT Mitarbeiter



„The cost of not doing IPv6 is great“

Jim Bound

Vielen Dank für Ihre Aufmerksamkeit

