IPv6 in der Praxis:
Microsoft Direct Access

Über mich

Thorsten Raucamp

- IT-Mediator
- Berater Infrastruktur / Strategie KMU
- Projektleiter,
  spez. Workflowanwendungen im Microsoft-Umfeld

- E-Mail: tr@raucamp-consulting.de

Web: www.raucamp-consulting.de

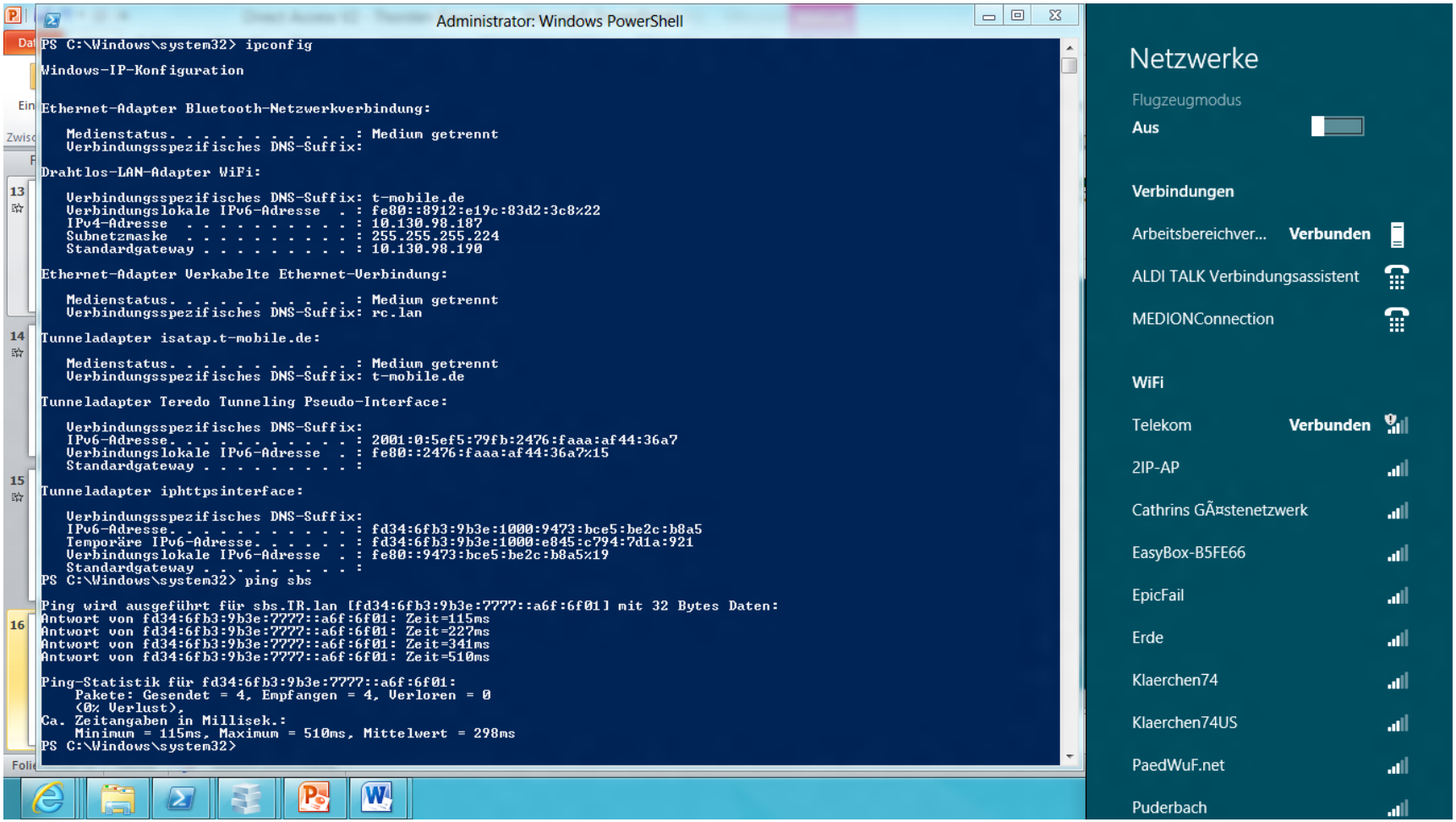
Agenda

- Was ist DirectAccess
- Voraussetzungen Version 2008 / 2012
- Minimal-Installation In 3 Schritten eingerichtet
- DirectAccess Security: von KMU bis Enterprise
- Fazit

Was ist Direct Access

- Transparenter und sicherer Remotezugriff ohne VPN-Zwang
- Automatischer Verbindungsaufbau vor der Benutzeranmeldung
- Client Remote Verwaltung, selbst wenn kein Benutzer angemeldet ist.
- IP-HTTPS: SSL/TLS-Verbindung wird zwischen Client und Server hergestellt, IP-Traffic mit IPSec verschlüsselt

Demo


Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig
Windows-IP-Konfiguration
Ethernet-Adapter Bluetooth-Netzwerkverbindung:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix:
Drahtlos-LAN-Adapter WiFi:
Verbindungsspezifisches DNS-Suffix: t-mobile.de
Verbindungslokale IPv6-Adresse . : fe80::8912:e19c:83d2:3c8%22
IPv4-Adresse . . . . . : 10.130.98.187
Subnetzmaske . . . . . : 255.255.255.224
Standardgateway . . . . . : 10.130.98.190
Ethernet-Adapter Verkabelte Ethernet-Verbindung:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix: rc.lan
Tunneladapter isatap.t-mobile.de:
Medienstatus. . . . . : Medium getrennt
Verbindungsspezifisches DNS-Suffix: t-mobile.de
Tunneladapter Teredo Tunneling Pseudo-Interface:
Verbindungsspezifisches DNS-Suffix:
IPv6-Adresse. . . . . : 2001:0:5ef5:79fb:2476:faaa:af44:36a7
Verbindungslokale IPv6-Adresse . : fe80::2476:faaa:af44:36a7%15
Standardgateway . . . . . :
Tunneladapter iphttpsinterface:
Verbindungsspezifisches DNS-Suffix:
IPv6-Adresse. . . . . : fd34:6fb3:9b3e:1000:9473:bce5:be2c:b8a5
Temporäre IPv6-Adresse. . . . . : fd34:6fb3:9b3e:1000:e845:c794:7d1a:921
Verbindungslokale IPv6-Adresse . : fe80::9473:bce5:be2c:b8a5%19
Standardgateway . . . . . :
PS C:\Windows\system32> ping sbs
Ping wird ausgeführt für sbs.TR.lan [fd34:6fb3:9b3e:7777::a6f:6f01] mit 32 Bytes Daten:
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=115ms
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=227ms
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=341ms
Antwort von fd34:6fb3:9b3e:7777::a6f:6f01: Zeit=510ms
Ping-Statistik für fd34:6fb3:9b3e:7777::a6f:6f01:
Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
(0% Verlust),
Ca. Zeitangaben in Millisek.:
Minimum = 115ms, Maximum = 510ms, Mittelwert = 298ms
PS C:\Windows\system32>
Netzwerke
Flugzeugmodus
Aus
Verbindungen
Arbeitsbereichver... Verbunden
ALDI TALK Verbindungsassistent
MEDIONConnection
WiFi
Telekom Verbunden
2IP-AP
Cathrins GÃ¤stenetzwerk
EasyBox-B5FE66
EpicFail
Erde
Klaerchen74
Klaerchen74US
PaedWuF.net
Puderbach

Agenda

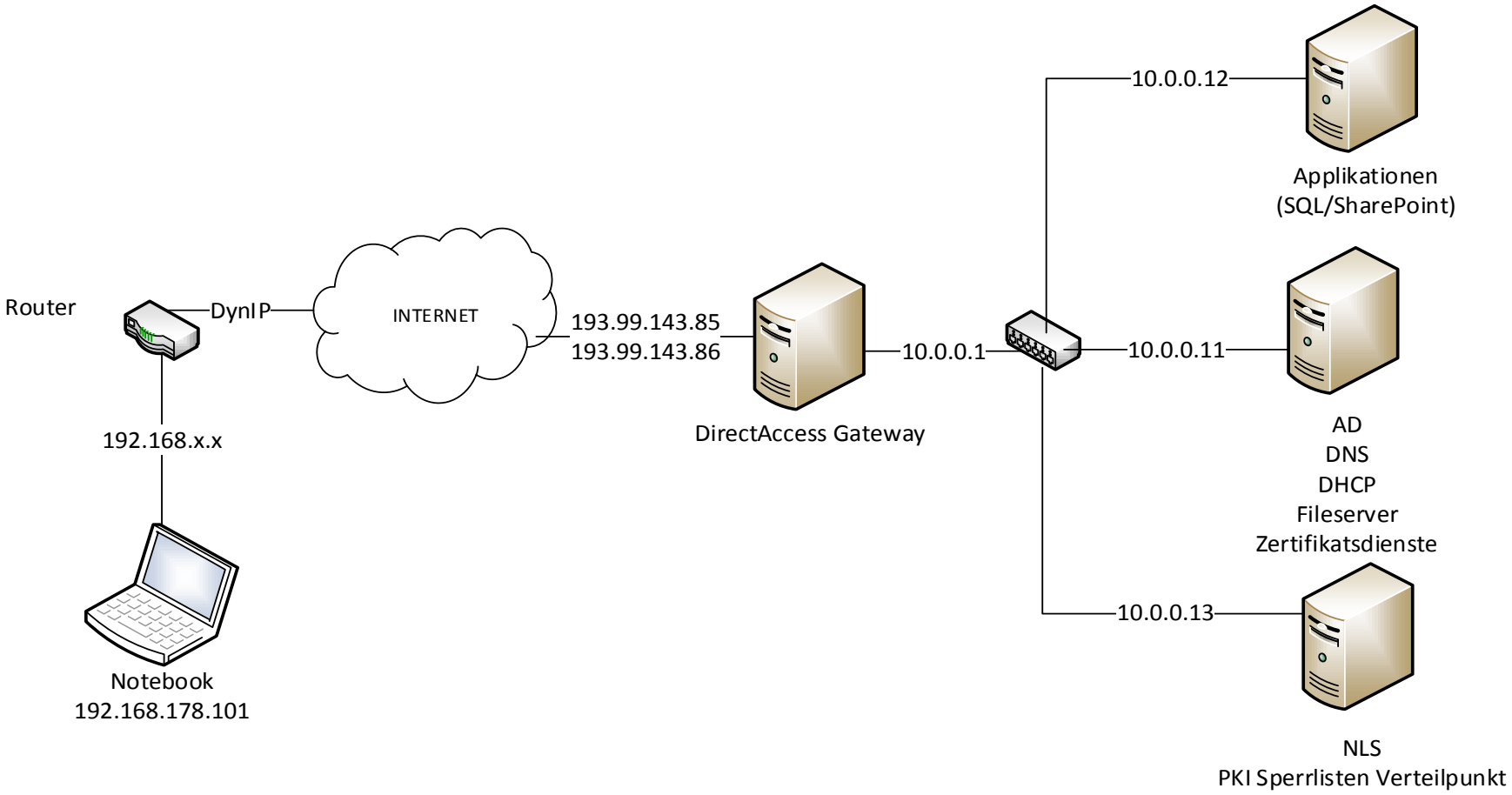
- Was ist Direct Access
- Voraussetzungen Version 2008 / 2012
- Minimal-Installation In 3 Schritten eingerichtet
- Direct Access Security: für jeden was dabei
- Fazit

DirectAccess in Windows 2008 R2

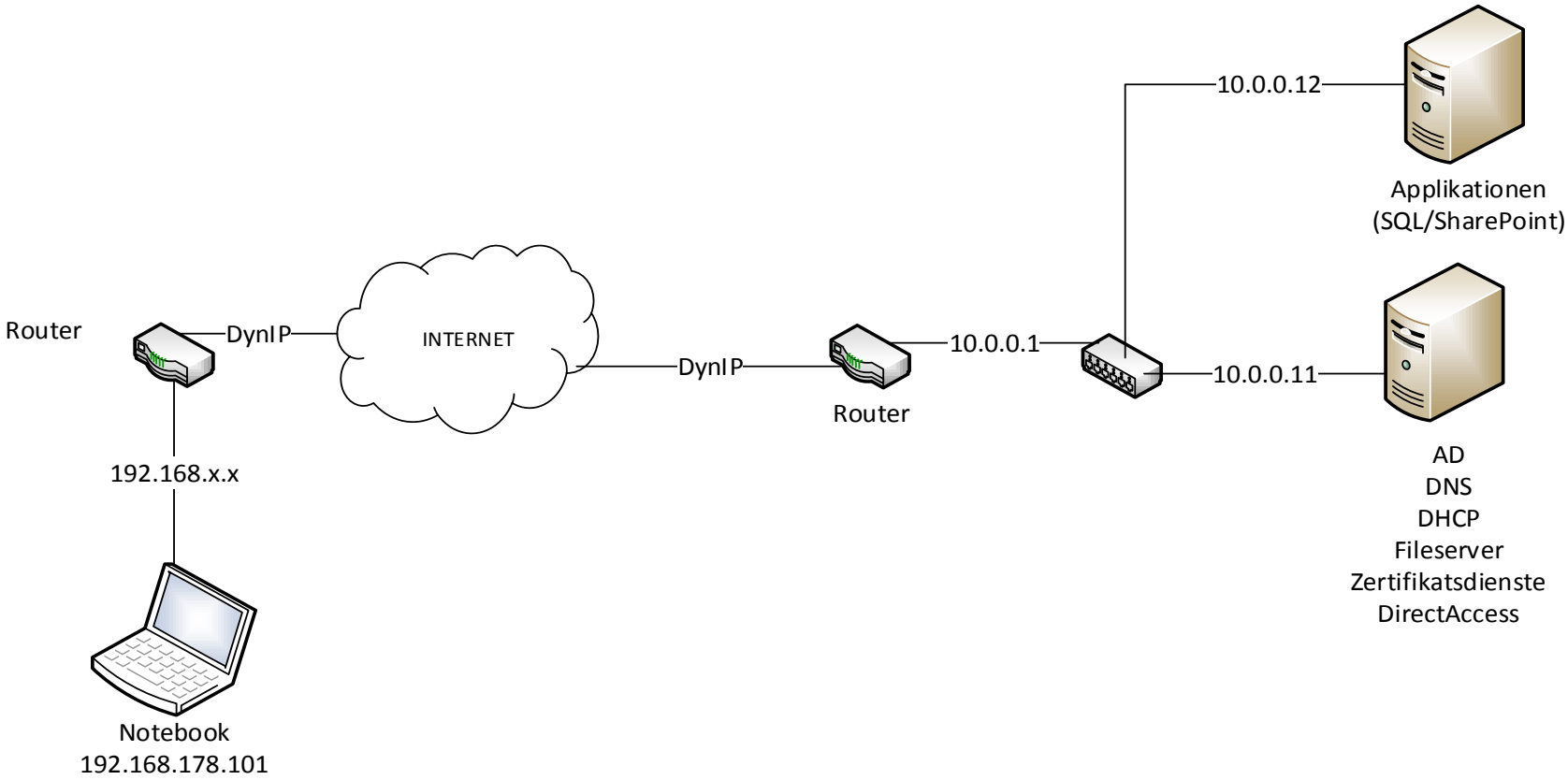
Anforderungen:

- DirectAccess Server (Server 2008 R2) mit 2 Netzwerkkarten
- Clients: Windows 7 (Ultimate / Enterprise)
- Public-Key Infrastruktur
- Firewall muss Teredo-Pakete durchlassen
- ISATAP-Infrastruktur einrichten
- NAT64 für IPv4 Ressourcen muss installiert und konfiguriert werden
- **2 öffentliche, aufeinander folgende IPv4-Adressen**

DirectAccess in Windows 2008 R2



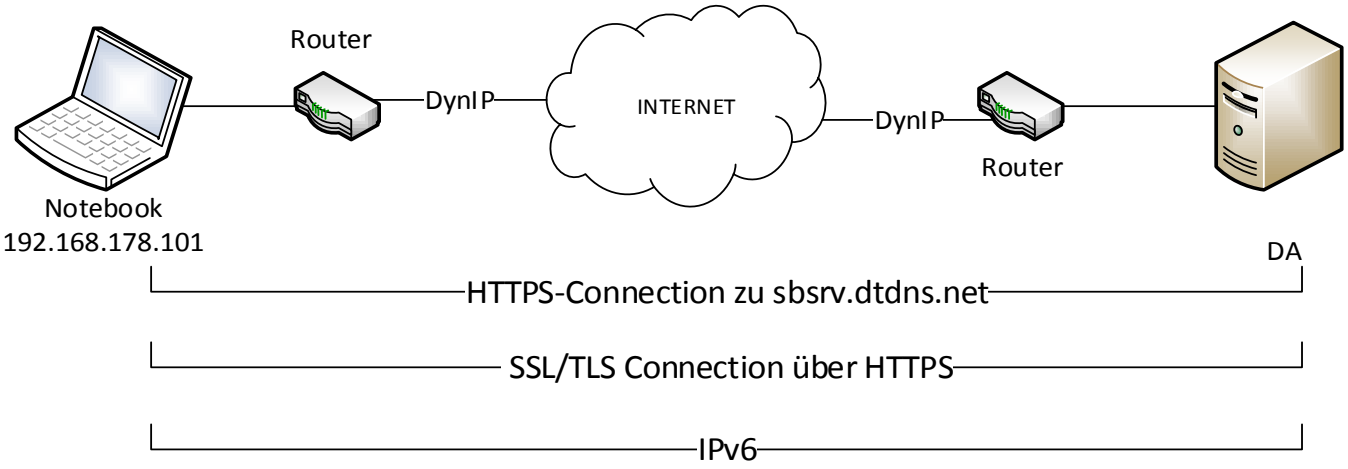
DirectAccess in Windows 2012



Verbesserungen in Server 2012

- DirectAccess Server hinter Firewall
- Vereinfachte Bereitstellung und Konfiguration
- Installation auf DC möglich (nicht empfohlen)
- Verbesserte Performance (insb. mit Win 8 Clients)
- Größere Skalierbarkeit
  (Unterstützung von Network Load Balancing)
- Unterstützung mehrerer Standorte
- DNS64 und NAT64 (Zugriff auf IPv4-Only Netze)

IP-HTTPS



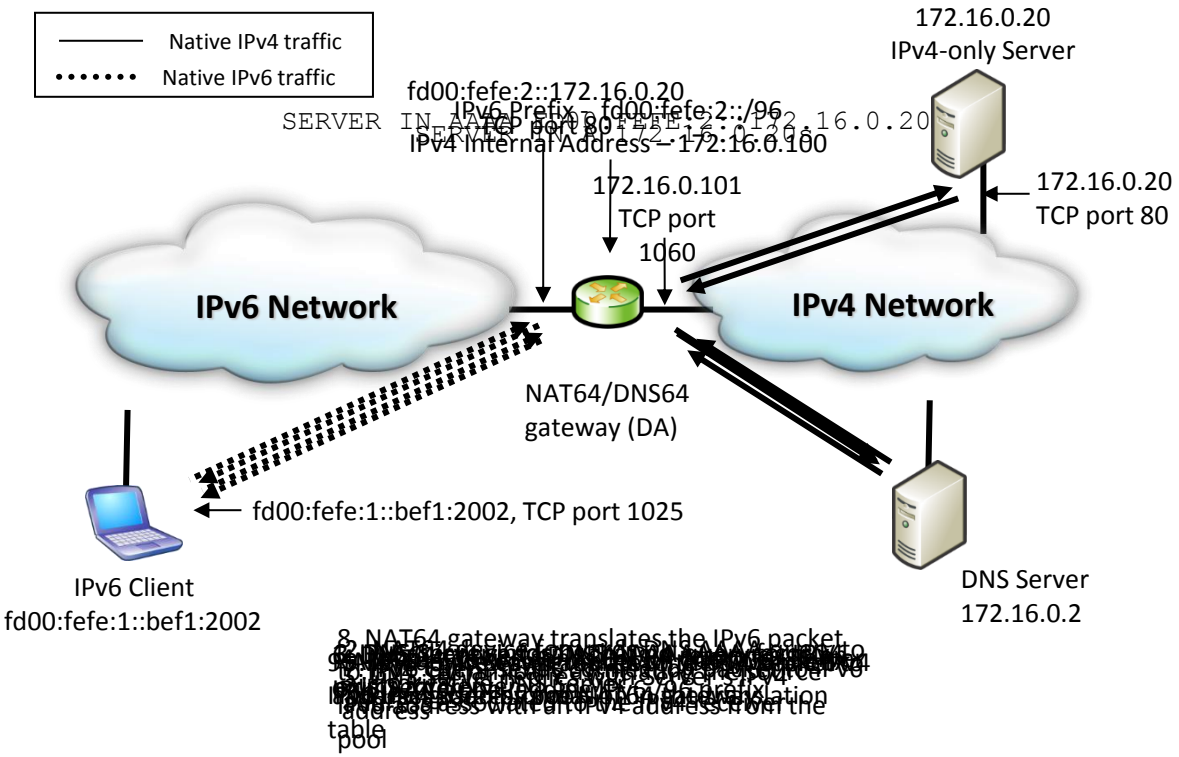
Automatischer Aufbau sobald Internet-Verbindung besteht

Windows 8: SSL-Tunnel ohne Verschlüsselung

2 Wege Kommunikation: Benutzerzugriff und Remote-Management

Technical Detail: NAT64/DNS64

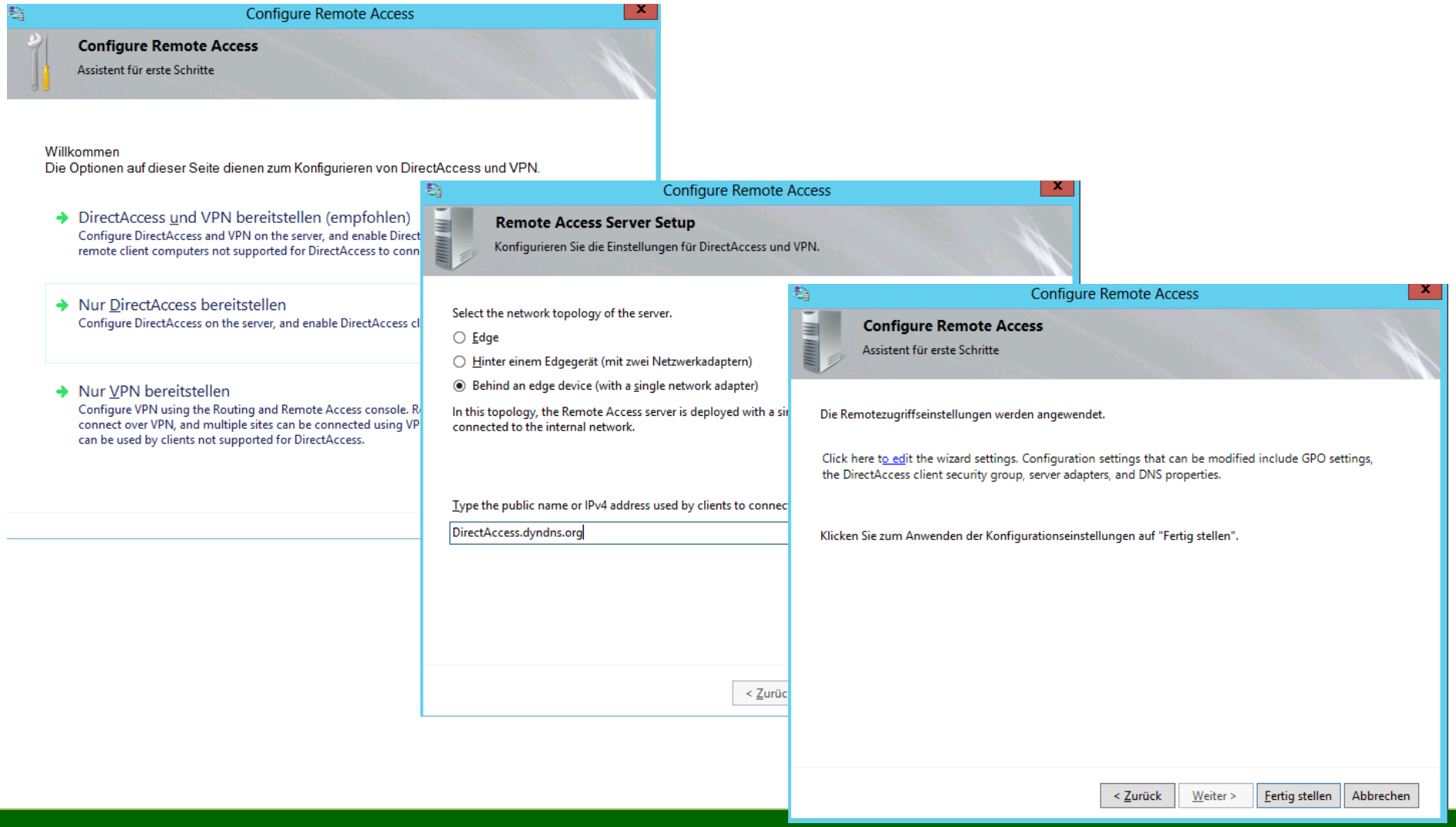
NAT64/DNS64 is the reason DA works on IPv4 Networks



Agenda

- Was ist Direct Access
- Voraussetzungen Version 2008 / 2012
- Minimal-Installation In 3 Schritten eingerichtet
- Direct Access Security: für jeden was dabei
- Fazit

In 3 Schritten zu DirectAccess



… Na ja, nicht ganz:

- Die restliche Infrastruktur muss richtig eingerichtet sein:
  - Firewall (Port 443 forwarding)
  - Active Directory
  - Zertifikatsdienste
  - DHCP
  - IPv6 ganz oder gar nicht!
  - **DNS** !!!

Agenda

- Was ist Direct Access
- Voraussetzungen Version 2008 / 2012
- Minimal-Installation In 3 Schritten eingerichtet
- Direct Access Security: für jeden was dabei
- Fazit

Security

- Plug‘n Pray ohne PKI
- Zertifikate, Smartcards und virtuelle Smartcards (TPM)
- OTP-Unterstützung (Token-Basierte Authentifizierung)
- NAP-Unterstützung
- Tunnelerzwingung möglich

Enterprise Features und Skalierung

- Remote-Verwaltung der Clients

- Einheitliche Verwaltung von Direct Access und RRAS
- Lastenausgleichsunterstützung / Clusterfähig
- Unterstützung mehrerer Standorte (Multisite Deployment)

Enterprise Features und Skalierung

- Einheitliche Verwaltung von Direct Access und RRAS
- Remote-Verwaltung der Clients
- Lastenausgleichsunterstützung / Clusterfähig
- Unterstützung mehrerer Standorte (Multisite Deployment)

Agenda

- Was ist Direct Access
- Voraussetzungen Version 2008 / 2012
- Minimal-Installation In 3 Schritten eingerichtet
- Direct Access Security: für jeden was dabei
- Fazit

Fazit:

- Technik wie sie sein sollte:
  - transparent für den Benutzer
  - gut administrierbar
  - skalierbar auf die jeweiligen Bedürfnisse

Vielen Dank für Ihre Aufmerksamkeit!