DNSSEC Validierung unter Windows

Ein Blick aus dem Fenster

MEN&MICE

DNSSEC unter Windows

- Bordmittel (aka Windows DNS Server 2008R2)
- gbDNS
- BIND
- Unbound

Windows 2008R2 DNS

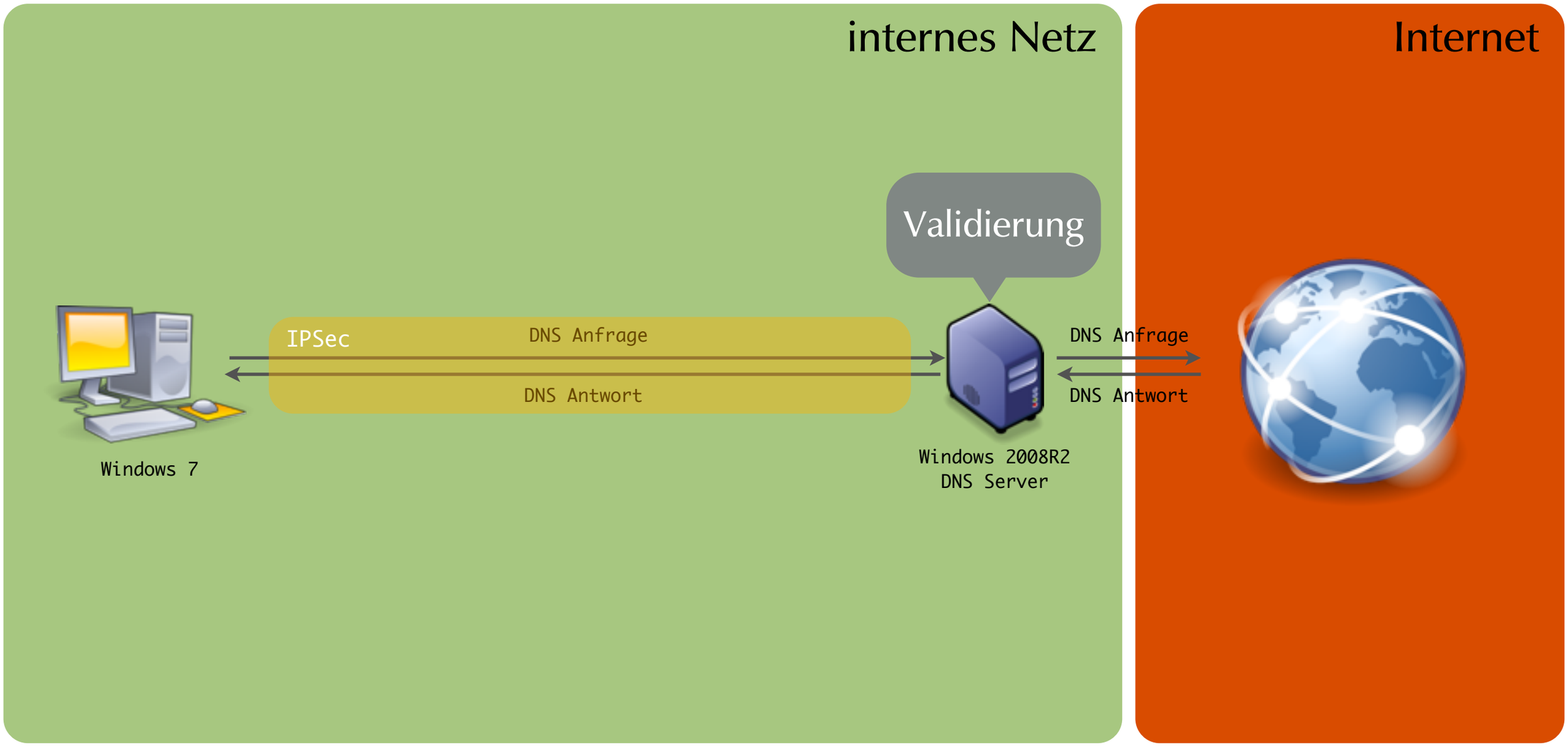
- Windows 2008R2 ist das aktuelle Server Betriebssystem der Firma Microsoft
  - erhältlich seit Oktober 2009
- Unterstützt DNSSEC nach RFC 4033/4034/4035
  - DNSSEC Zone-signing
  - DNSSEC Validierung

Windows 2008R2 DNS

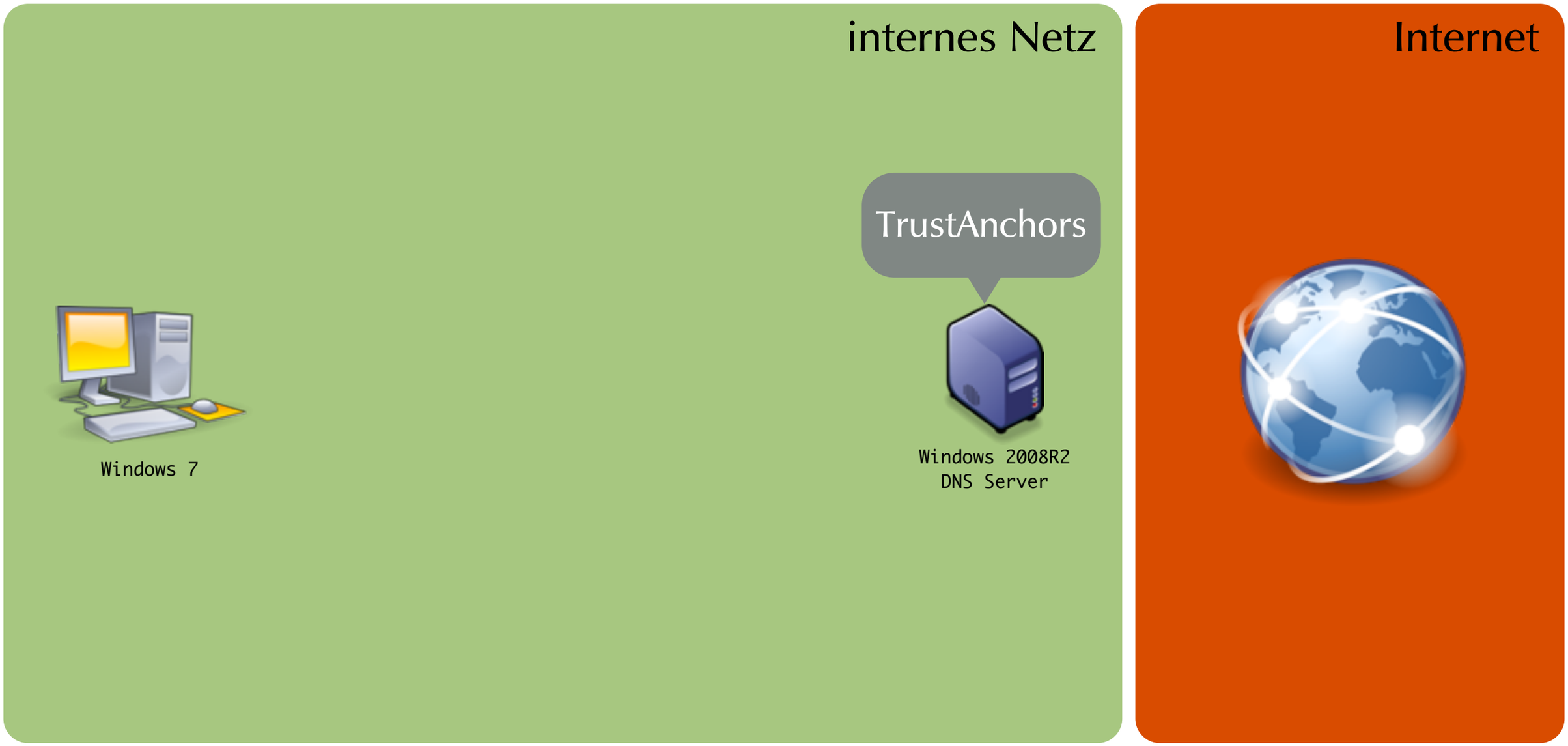
- **nicht** unterstützt in der aktuellen Version (2008R2SP1rc1) vom Oktober 2010 sind

- NSEC3
- andere DNSSEC Algorithmen ausser SHA1 (kein SHA256, GOST ...)
- DNSSEC lookaside validation (DLV)

Windows 2008R2 DNS



Windows 2008R2 DNS



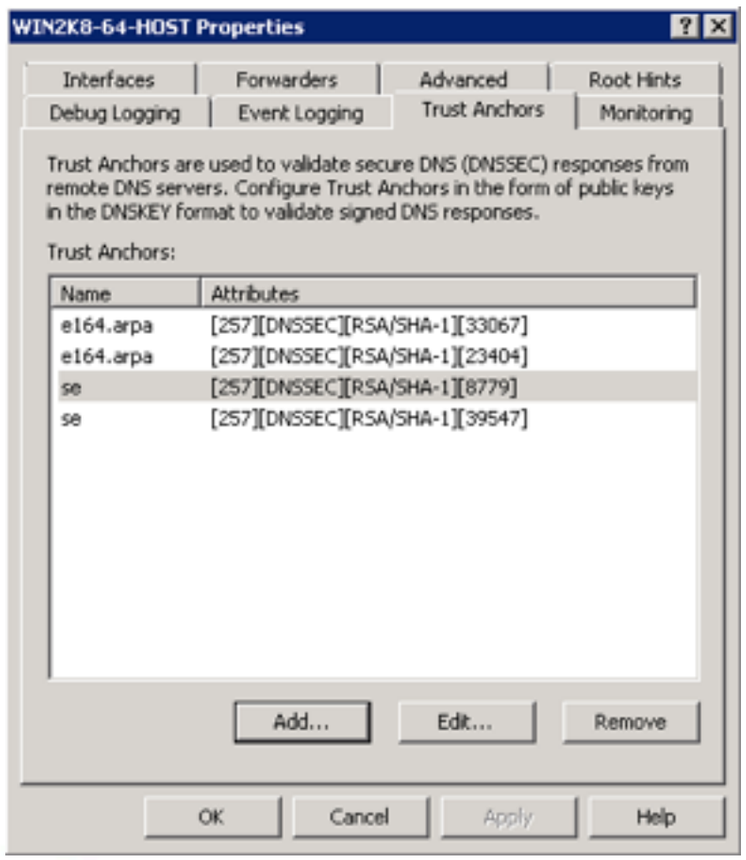
Windows 2008R2 DNS

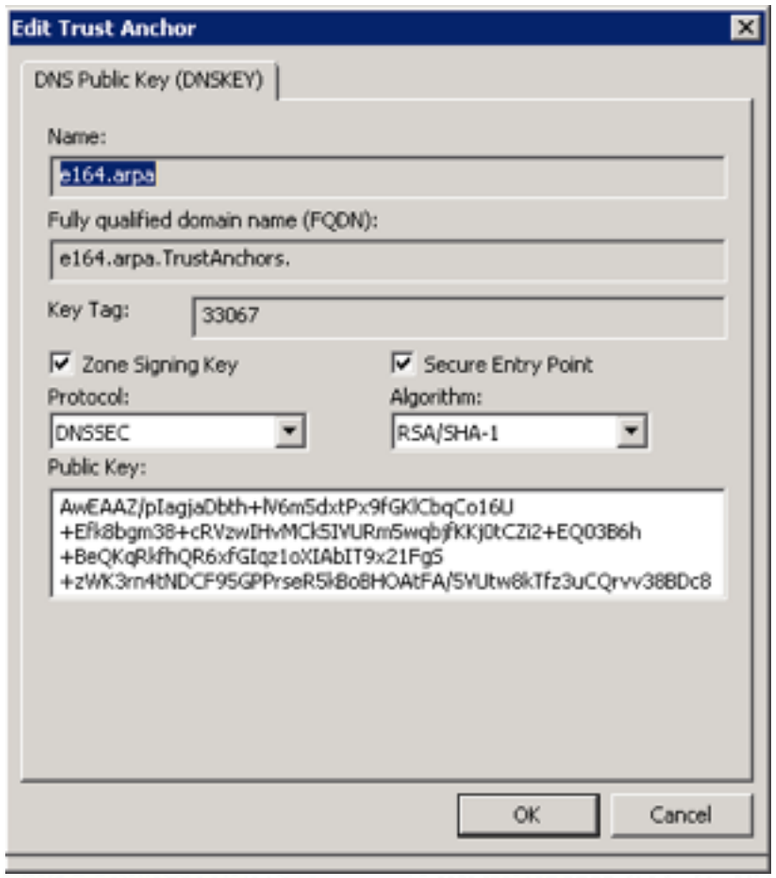
- Trust Anchor für Zonen können per GUI oder per Kommandozeile eingepflegt werden

```
C:\bind>dnscmd /TrustAnchorAdd se DNSKEY 257 3 5 AwEAAbaxTum9L7z1DmPiXPk0QZ2/qUM
3to210Caey/ycZuvQ8Mh/dgGpwBmyZB9xZSkaCLa2Mw6pmDLrjK9hWOffq5PXRVm9RrcA/eIEBEvbQzk
Y5sFkWAczNAs58Oscxi+/Gd5KfuVi3lJpYgJwwa2JB4doZ00IXywcCn0VTz0Hsl/lqpA2Bqj+e+ATzA5
hWyiNyHPjiYvyMCkSXTiGgFVVuG8H3N6Us8uSABuO2UoFQeQi6YikIiCbf1FfCzr4vBIRXW6MaDs8kqA
AadKjLk3i39dviL/YeyGUvq9Dan9PsvkwQejKN/7J0yCr2nYXfwGGCHkcBKkagv79EaR1ZigUCp8=

Command completed successfully.
```

Windows 2008R2 DNS

- Trust Anchor für Zonen können per GUI oder per Kommandozeile eingepflegt werden





Windows 2008R2 DNS

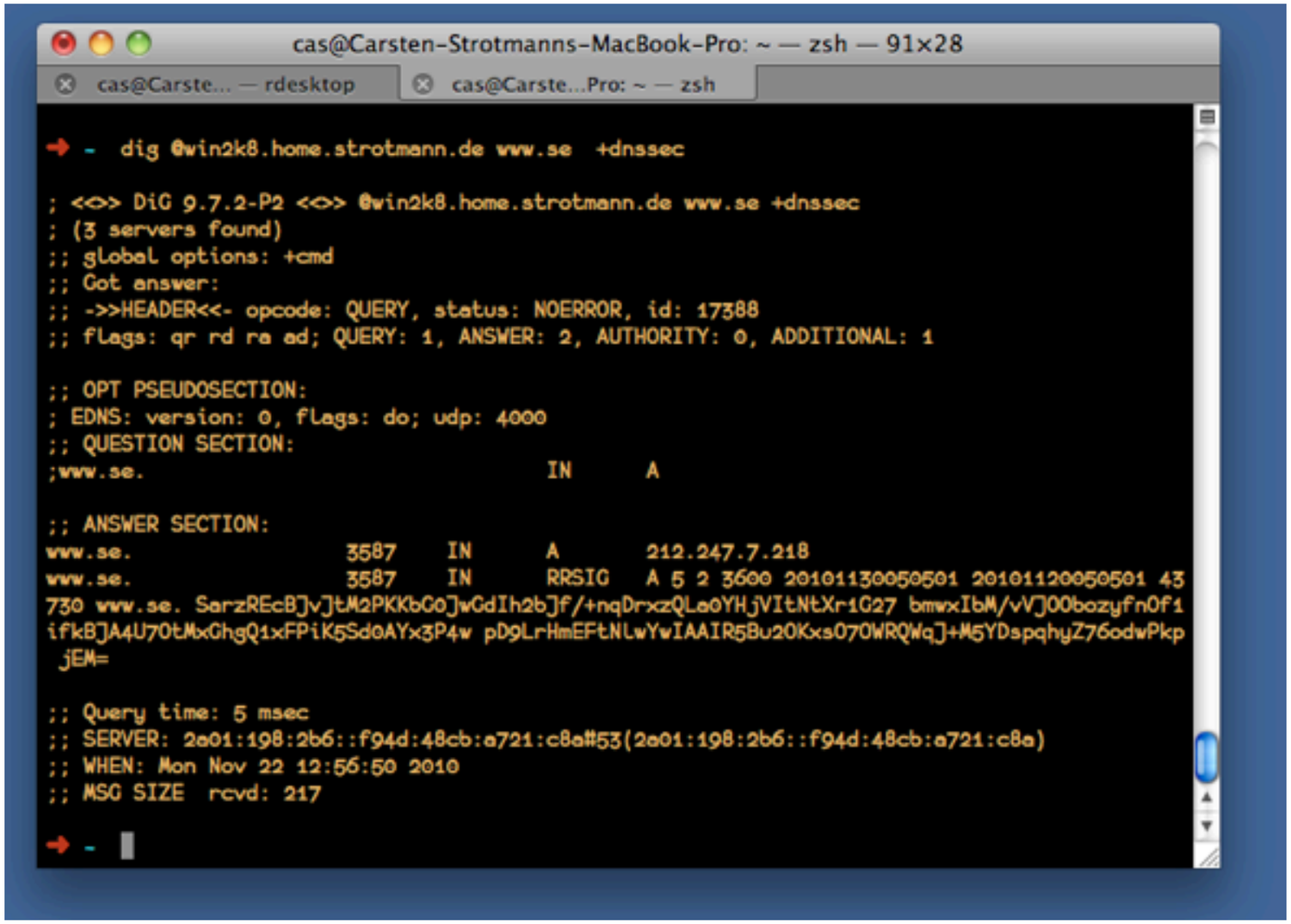
- Trust Anchors werden in einer Zonen-Datei unter `%WINDIR%/System32/dns/TrustAnchors.dns` gespeichert

Windows 2008R2 DNS

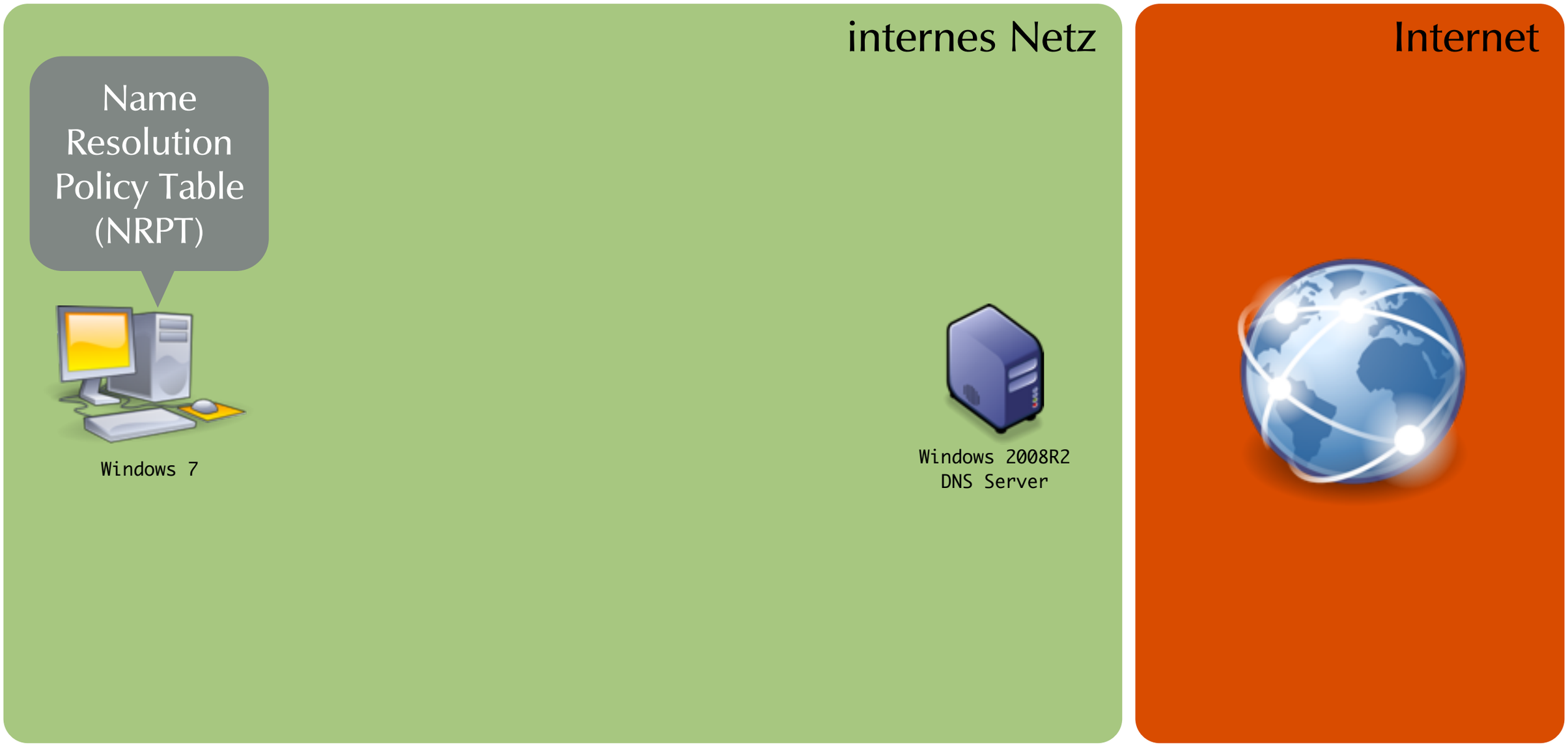
- eine lokale TLD namens “TrustAnchors”

```
~  dig @win2k8r2 se.TrustAnchors DNSKEY
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.2-P2 <<>> @192.168.1.165 se.TrustAnchors DNSKEY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60618
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;se.TrustAnchors.           IN     DNSKEY

;; ANSWER SECTION:
se.TrustAnchors.     3600   IN     DNSKEY 257 3 5 AwEAAbax[...] EaRlZigUCp8=
se.TrustAnchors.     3600   IN     DNSKEY 257 3 5 AwEAAeeG[...] 9s9jakbWzd4PM1Q551XIEphRGyqcbA2JTU3/mcUVKfgrH7nxaPz5DoUB 7TKYyQgsTlc=

;; Query time: 2 msec
;; SERVER: 192.168.1.165#53(192.168.1.165)
;; WHEN: Mon Nov 22 14:54:51 2010
;; MSG SIZE  rcvd: 585
```

Windows 2008R2 DNS



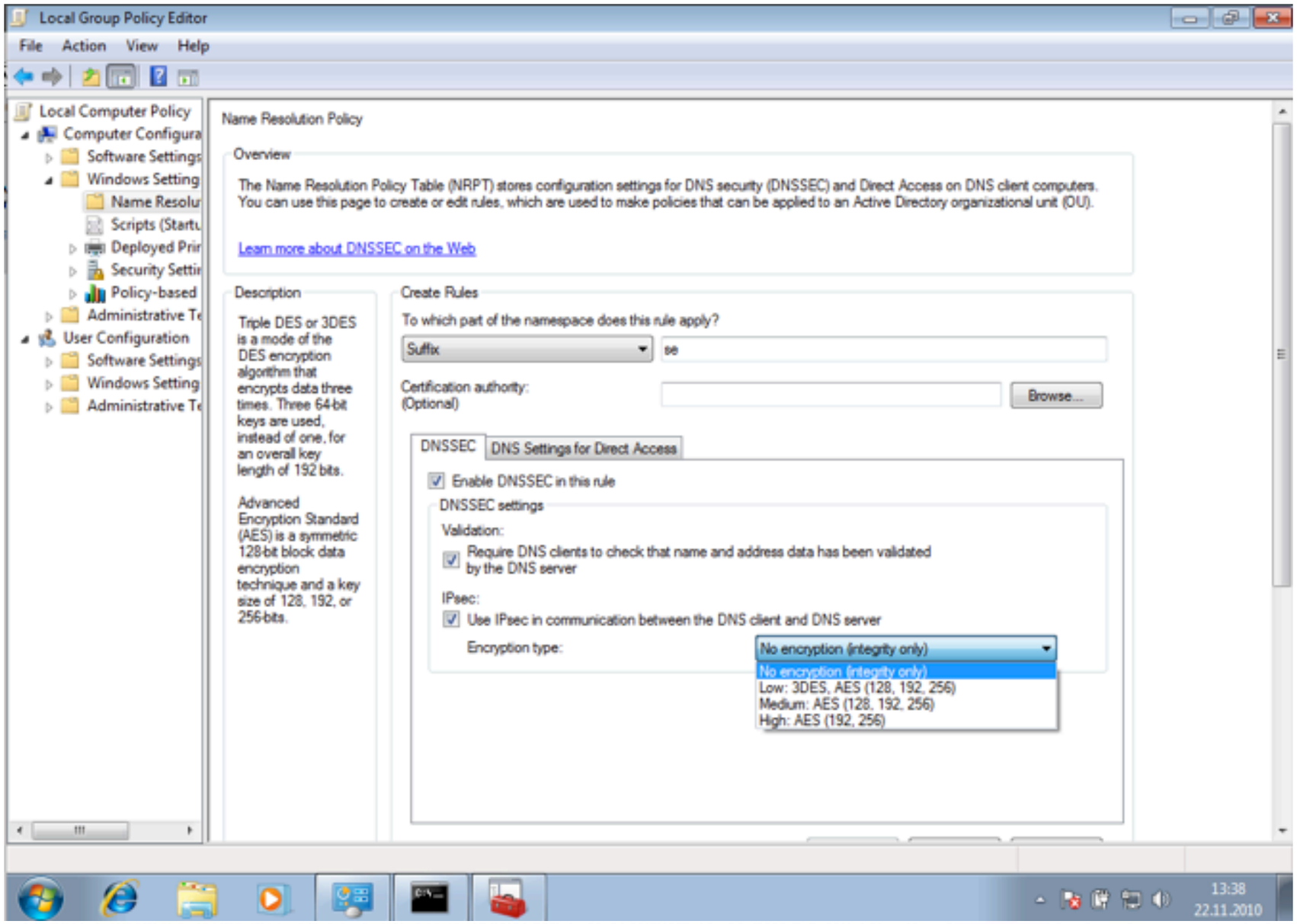
Windows 2008R2 DNS



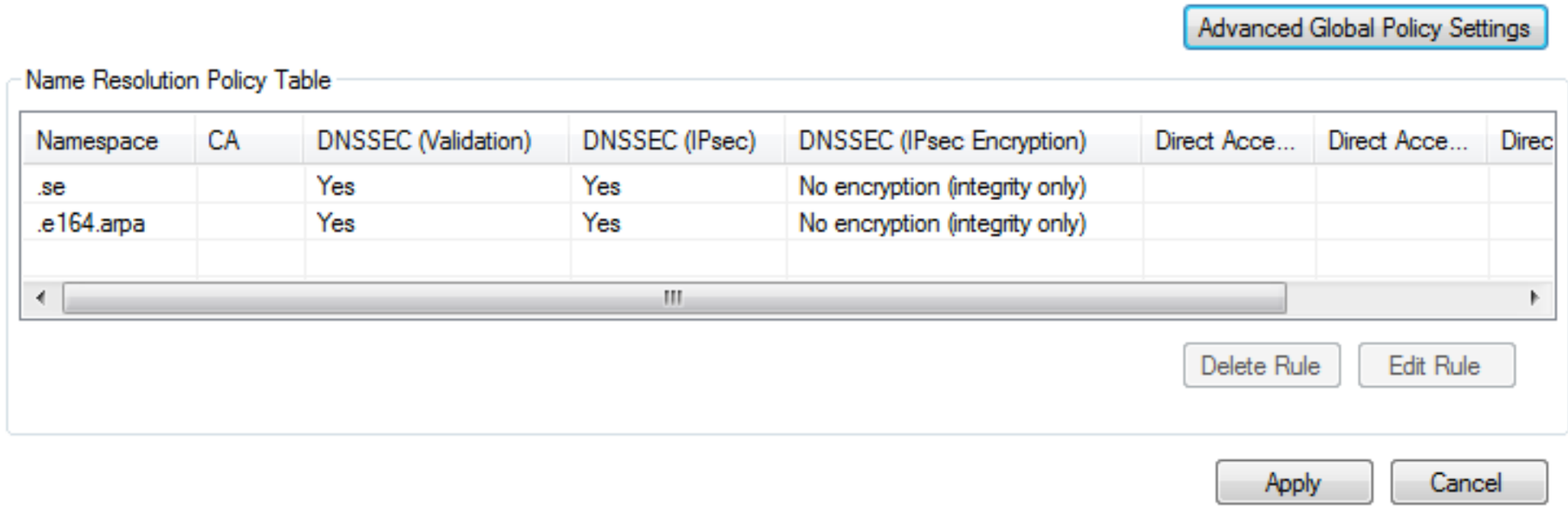
Windows 2008R2 DNS

- Auf DNS stub-resolvern (DNS Client) wird die Name-Resolution-Policy-Table (NRPT) gepflegt
  - die NRPT bestimmt...
    - ... für welche Domains wird DNSSEC Validierung angefragt (DO-Flag) und ein AD-Flag in der Antwort erwartet(!)
    - ... für welche Domains wird IPSec zwischen Client und DNS Server verwendet

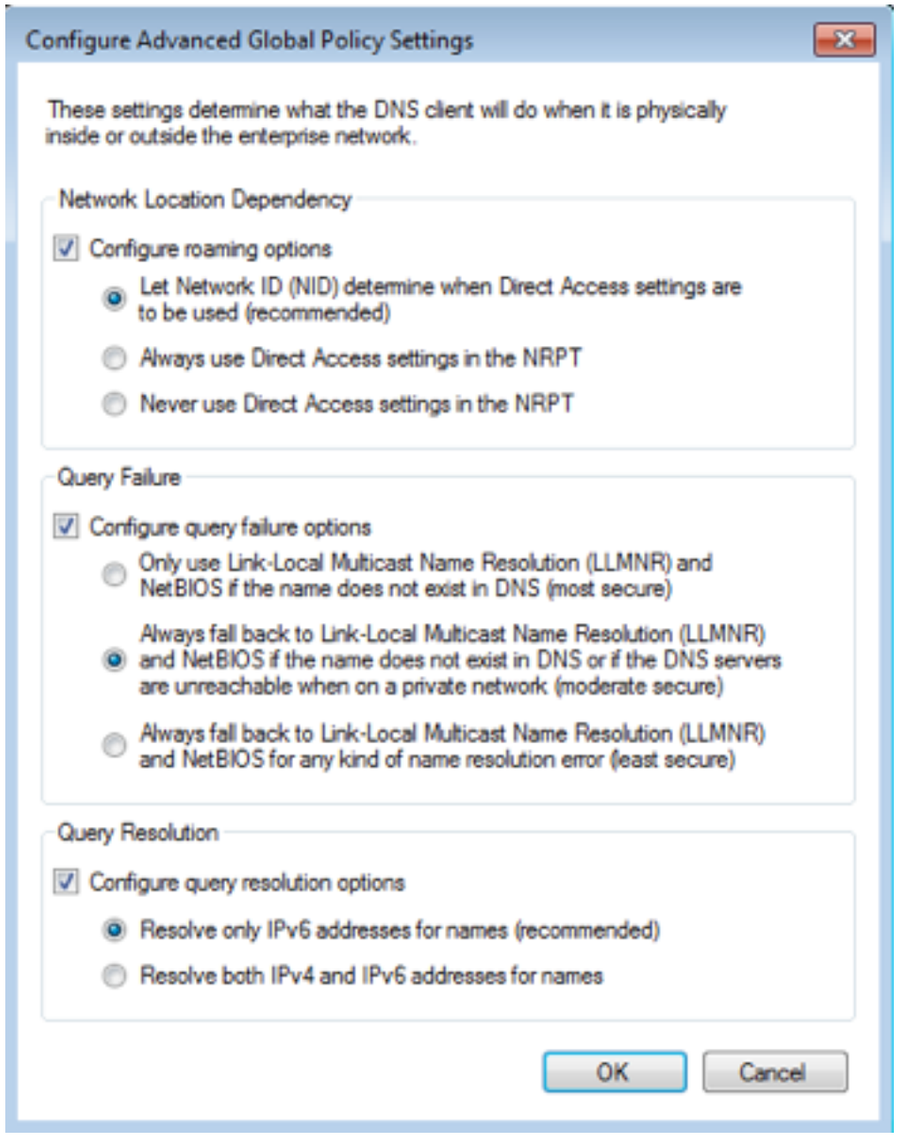
Windows 2008R2 DNS



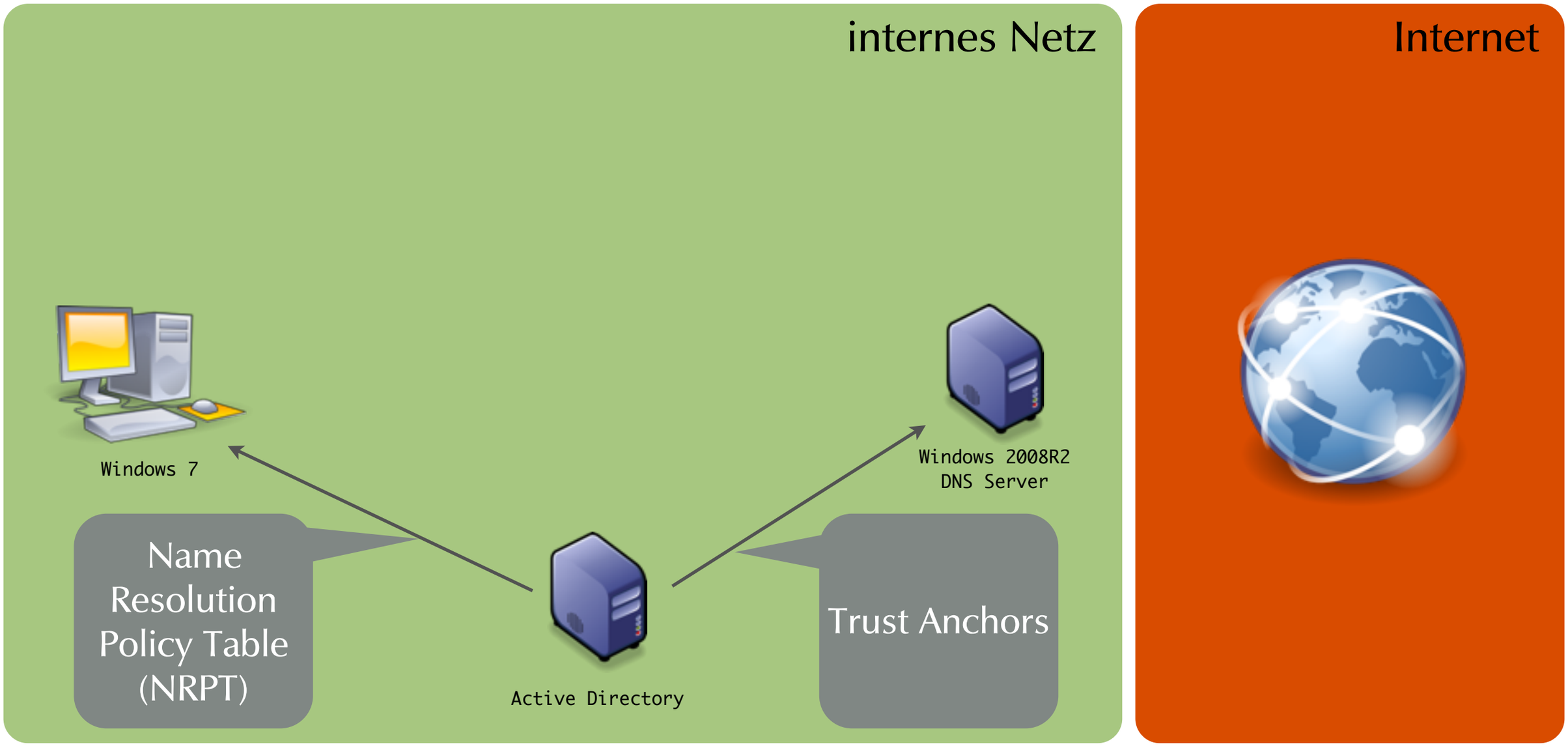
Windows 2008R2 DNS



Windows 2008R2 DNS



Windows 2008R2 DNS



Windows 2008R2 DNS

- Informationen:
  - DNSSEC deployment guide (Beta) for Windows Server 2008 R2, März 2010

    http://www.microsoft.com/downloads/details.aspx?FamilyID=7a005a14-f740-4689-8c43-9952b5c3d36f&DisplayLang=en

Alternativen

Alternativen

- BIND 9.7.x für Windows
  - http://www.isc.org/software/bind/972-p2/download/bind972-p2zip

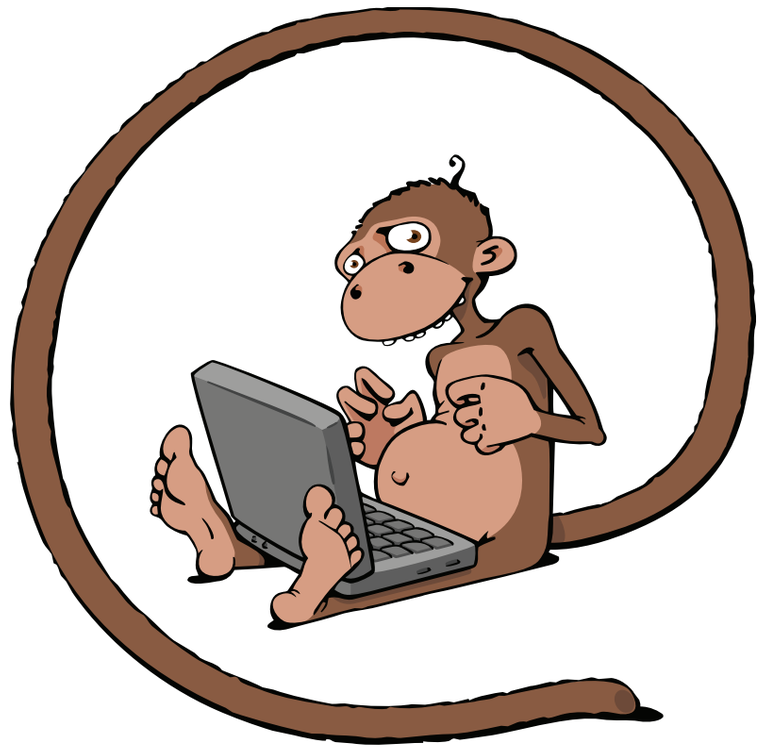
Alternativen

- Unbound 1.4.7 für Windows
  - `http://unbound.net/downloads/unbound_setup_1.4.7.exe`

Alternativen

- GbDns (George Barwood DNS)
  `http://www.george-barwood.pwp.blueyonder.co.uk/DnsServer/`
  - geschrieben in C#, .NET
  - keine externe Konfiguration (nur im Quellcode), keine GUI
  - Root-Trust-Anchor einkompiliert, validiert SHA256 und NSEC3
  - Recursion nur für private IP Netze (RFC 1918) + Loopback

Fragen?



Vielen Dank!

E-Mail:
carsten@menandmice.com

MEN&MICE