

DNSSEC Validierung unter Windows

Ein Blick aus dem Fenster



MEN&MICE

© Men & Mice <http://menandmice.com>

DNSSEC unter Windows

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

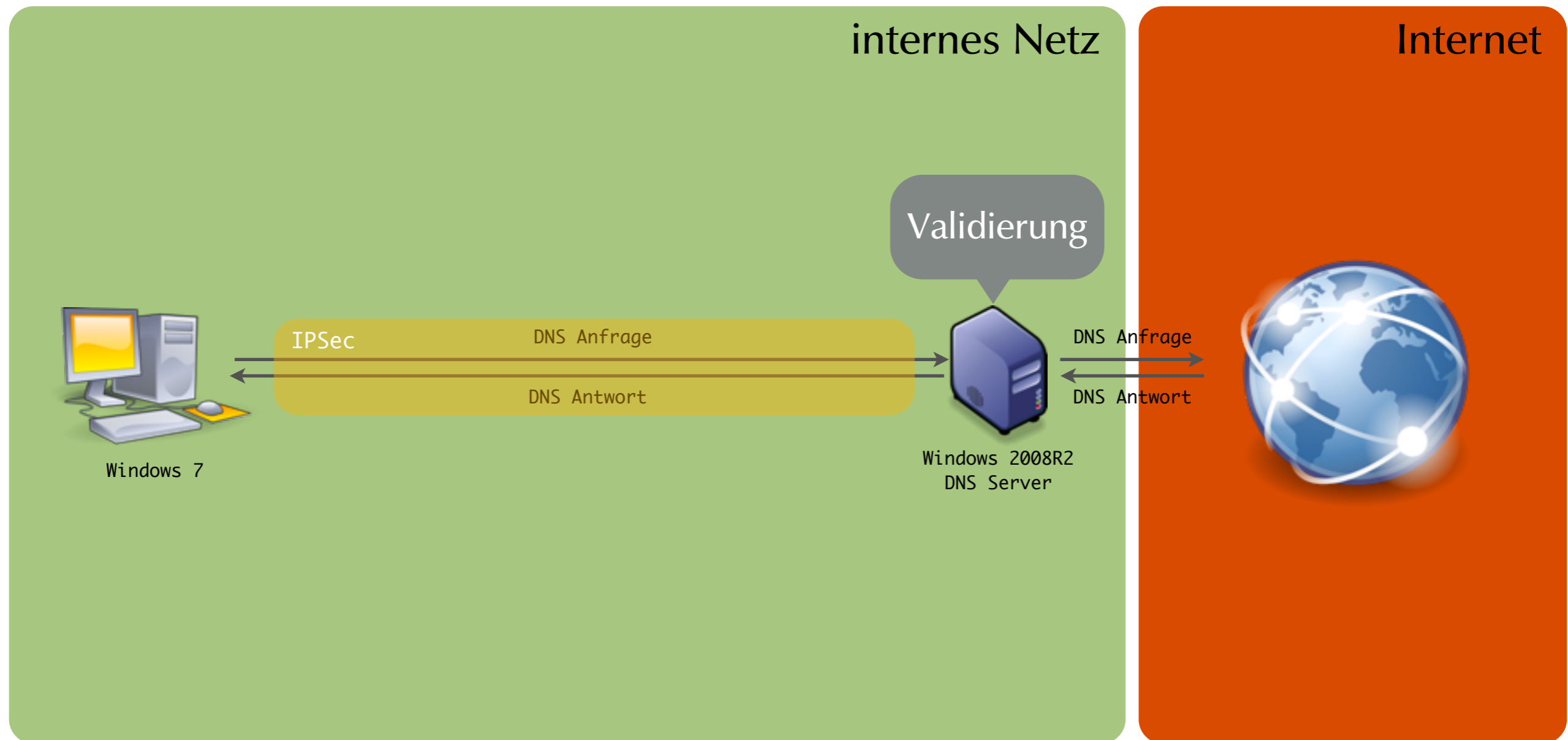
Windows 2008R2 DNS

- 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

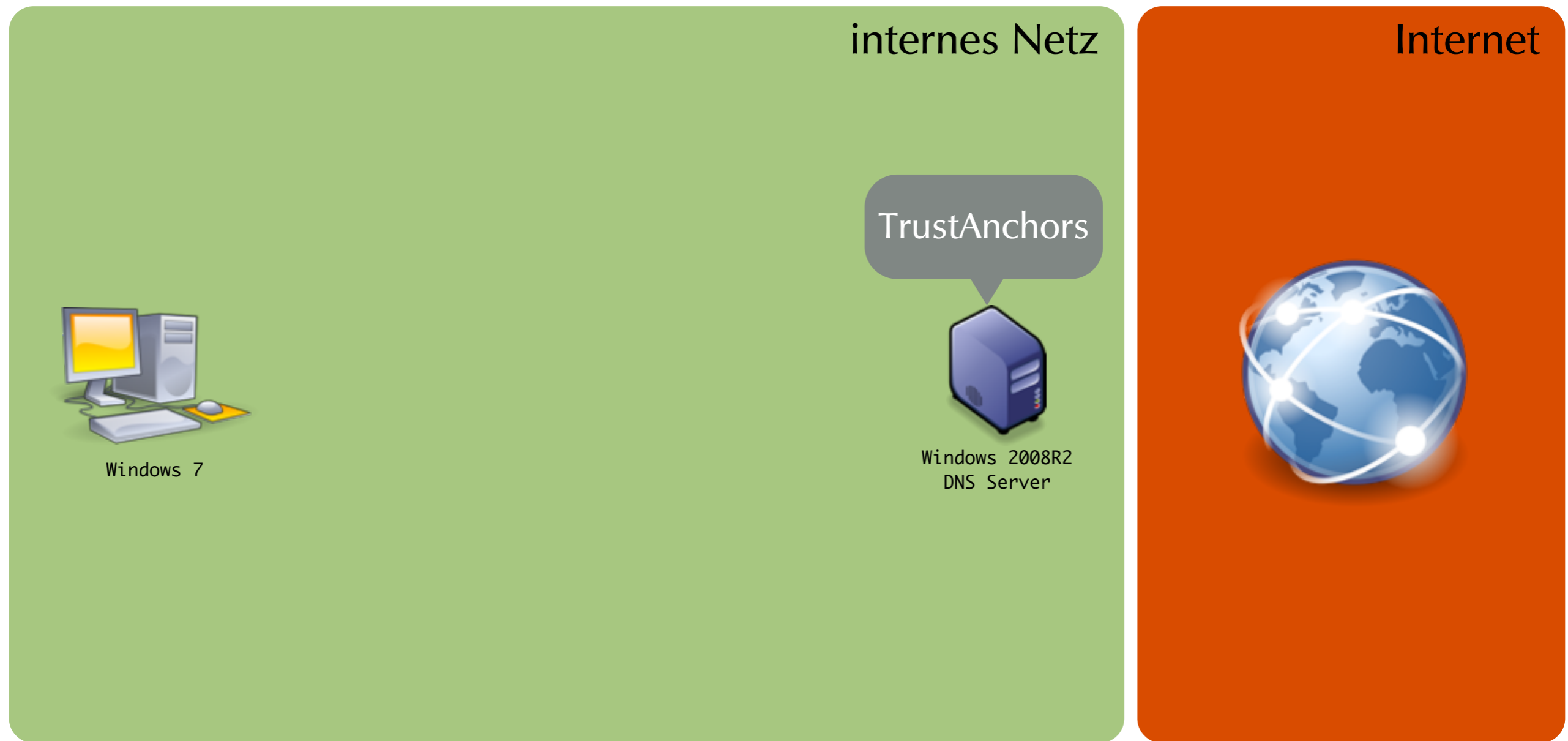
Windows 2008R2 DNS

- **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

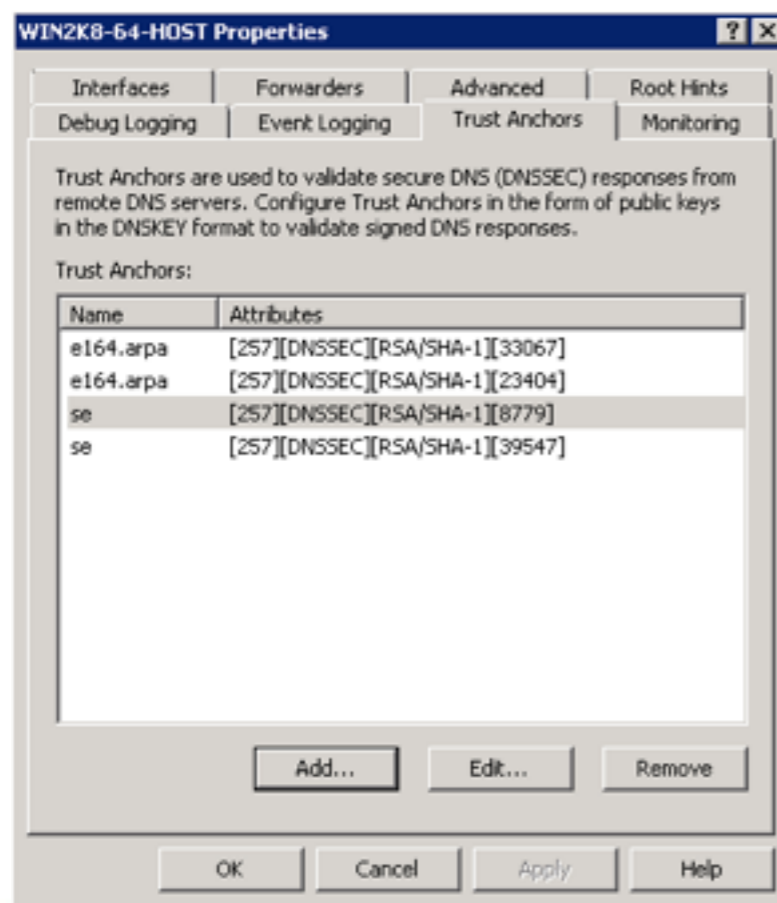
- Trust Anchor für Zonen können per GUI oder per Kommandozeile eingepflegt werden

```
C:\bind>dnscmd /TrustAnchorAdd se DNSKEY 257 3 5 AwEAAbaxTum9L7z1DmPiXPk0QZ2/qUM
3to210Caey/ycZuvQ8Mh/dgGpwBmyZB9xZSkaCLa2Mw6pmDLrjK9hWOffq5PXRUm9RrcA/eIEBEvbQzk
Y5sFkWAczNAs580scxi+/Gd5KfuUi3lJpYgJwwa2JB4doZ00IXywcCn0UTz0Hs1/lqpA2Bqj+e+ATzA5
hWyiNyHPjiYvyMCkSXTiGgFUUuG8H3N6Us8uSABu02UoFQeQi6YikIiCbf1FfCzr4vBIRXW6MaDs8kqA
AadKjLk3i39dviL/YeyGUvq9Dan9PsvkwQejKN/7J0yCr2nYXfwGGCHkcBkkagv79EaRlZigUCp8 =

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

```
TrustAnchors.dns - Notepad
File Edit Format View Help
Database file TrustAnchors.dns for TrustAnchors zone.
Zone version: 11
.....
IN SOA w1n2k8-64-host.home.strotmann.de. hostmaster.home.strotmann.de. (
    11          : serial number
    900        : refresh
    600        : retry
    86400     : expire
    3600      : default TTL
)
.....
Zone NS records
.....
NS w1n2k8-64-host.home.strotmann.de.
.....
Zone records
e164.arpa
DNSKEY 257 3 5 {
AwEAAZgUwRPePSHESUkqWfZaxkk0en4E2v8
1gu1ku1R8eb0xqy0Ujfo1M51N29ndqofayQ
u2e3APx9LR8ccnd5Gw8sgwu7v1Drqapgbx
xzCTf93D+1evC7z5BLVzV06yyGC2rGsgMAx
zw2efrv7Rj1R5vgr6mq0R5rZfCCya2uI103G
CHKfBbmF56PpgkD8EbUPkd7JbM1/bwzprofb
dLYthg2014FBNTnemnsxSMckRv+1B5sAfayv
5sPIC0SSRQL13F5MNVb+MqE+R200H/ANmkt
C/ZIHAZU2/J1E+obl5qtj5kudEef3LzAcwy
xv/gpawMqjpbndcyjzqc3c=
} : key tag = 23404
DNSKEY 257 3 5 {
AwEAAZ/pIagjadbth+lv6m5dxtPx9fGk1Cbq
Co16U+8Fk8Bgm3B+crvzwlHvMCK51vUrm5wq
bjfXk]0tC21+8Q03B8h+8eQkqkFhg8xfg
Iq21dXIABIT9x21Fg5+zwk3rn4tNDCF95GPP
rser5k80Bh0AtFA/5vutw8kTF23uCGrvv3BB
DcBI/w5TWKHu8J1DKEztj8GLwCQ+X+r8vdv
dkUyavf2vqM3N8kHbumM0h1J3aavRT2ox
8smg2blcaM]ruc18ZF5b5kC1Jdw3k8v1+acc
8wC2Mh250GxpwFQjHlUYR5v/94G0+wGTFM
1fZE/24Uq02PA2j44dWku=
} : key tag = 33067
rfpe.net
DNSKEY 257 3 5 {
AwEAAx7FvREPM1n1/ohenzgwbqpc2jcv0fyd
ccof9mwvynubrLwaxwFP21UgAMUEICxwI8z
f5N0Iut5wrJyYgokZxqHyCMcy5Z25GctDEj1
Zdhzqb1hq1v5n2qMhMfvqdgdw3ba8MhyBv8
```

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

```
cas@Carsten-Strotmanns-MacBook-Pro: ~ — zsh — 91x28
cas@Carste... — rdesktop  cas@Carste...Pro: ~ — zsh
→ - dig @win2k8.home.strotmann.de www.se +dnssec

; <<> DiG 9.7.2-P2 <<> @win2k8.home.strotmann.de www.se +dnssec
; (3 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17388
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

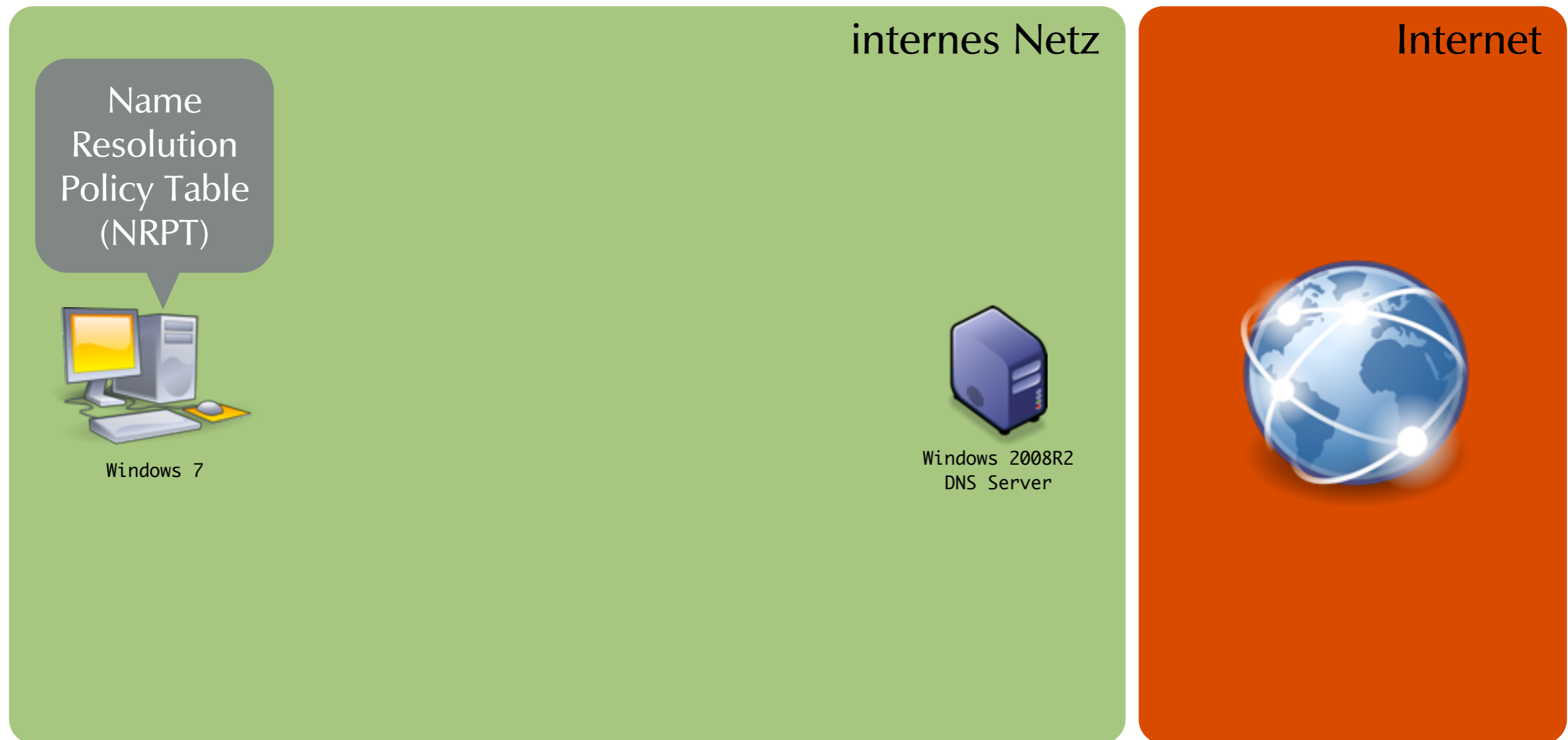
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4000
;; QUESTION SECTION:
;www.se.                IN      A

;; ANSWER SECTION:
www.se.                 3587    IN      A      212.247.7.218
www.se.                 3587    IN      RRSIG  A 5 2 3600 20101130050501 20101120050501 43
730 www.se. SarzREcBJvJtM2PKKbG0JwGdIh2bJf/+nqDrxczQLa0YHjVItNtXr1G27 bmwIbM/vVJ00bozyfn0f1
ifkBJA4U70tMxGhgQ1xFPiK5Sd0AYx3P4w pD9LrHmEFtNLwYwIAAIR5Bu20Kxs070WRQWqJ+M5YDspqhyZ76odvPkp
jEM=

;; Query time: 5 msec
;; SERVER: 2a01:198:2b6::f94d:48cb:a721:c8a#53(2a01:198:2b6::f94d:48cb:a721:c8a)
;; WHEN: Mon Nov 22 12:56:50 2010
;; MSG SIZE rcvd: 217

→ -
```

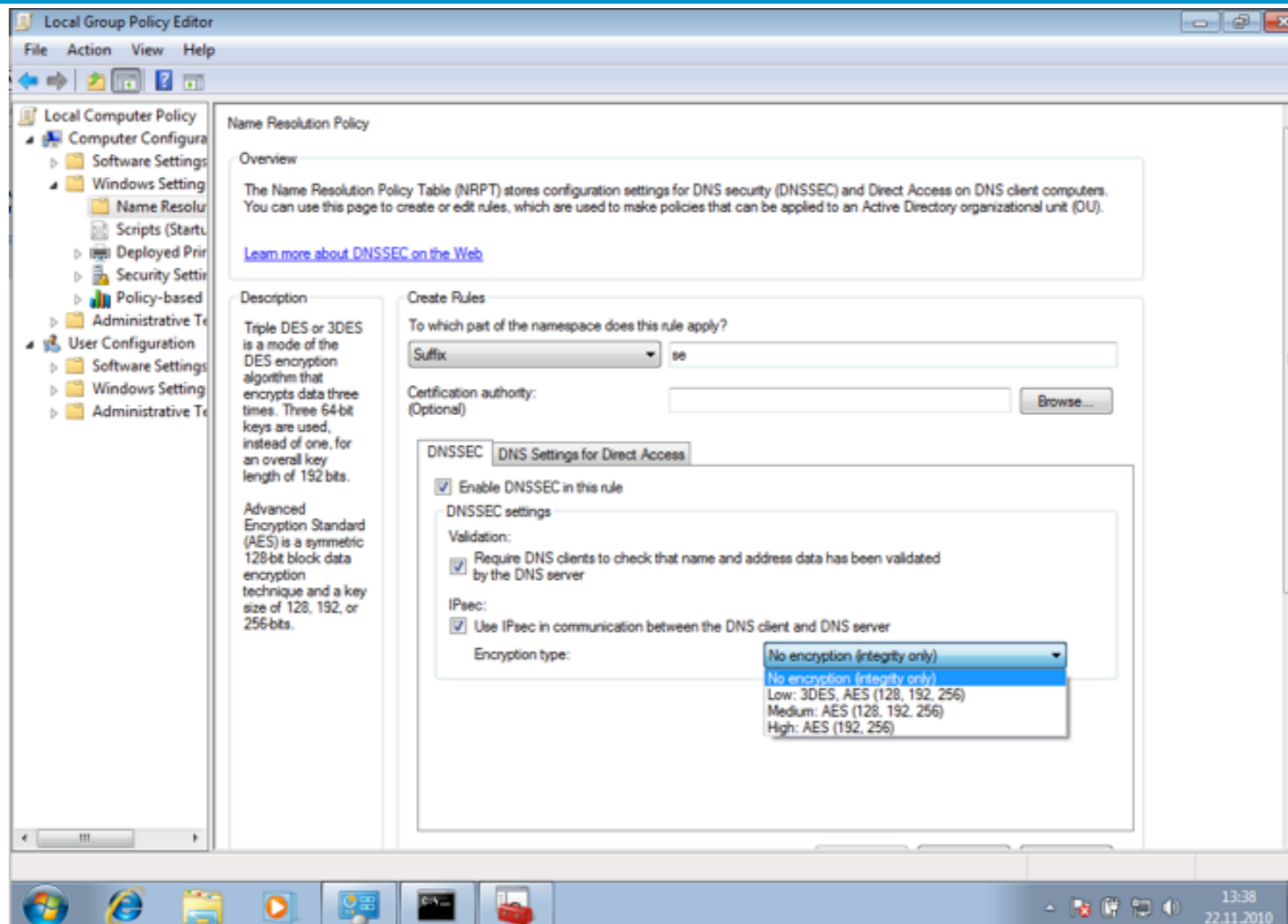
Windows 2008R2 DNS



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

Advanced Global Policy Settings

Name Resolution Policy Table

Namespace	CA	DNSSEC (Validation)	DNSSEC (IPsec)	DNSSEC (IPsec Encryption)	Direct Acce...	Direct Acce...	Dirac
.se		Yes	Yes	No encryption (integrity only)			
.e164.arpa		Yes	Yes	No encryption (integrity only)			

Delete Rule Edit Rule

Apply Cancel

Windows 2008R2 DNS

Configure Advanced Global Policy Settings

These settings determine what the DNS client will do when it is physically inside or outside the enterprise network.

Network Location Dependency

- Configure roaming options
 - Let Network ID (NID) determine when Direct Access settings are to be used (recommended)
 - Always use Direct Access settings in the NRPT
 - Never use Direct Access settings in the NRPT

Query Failure

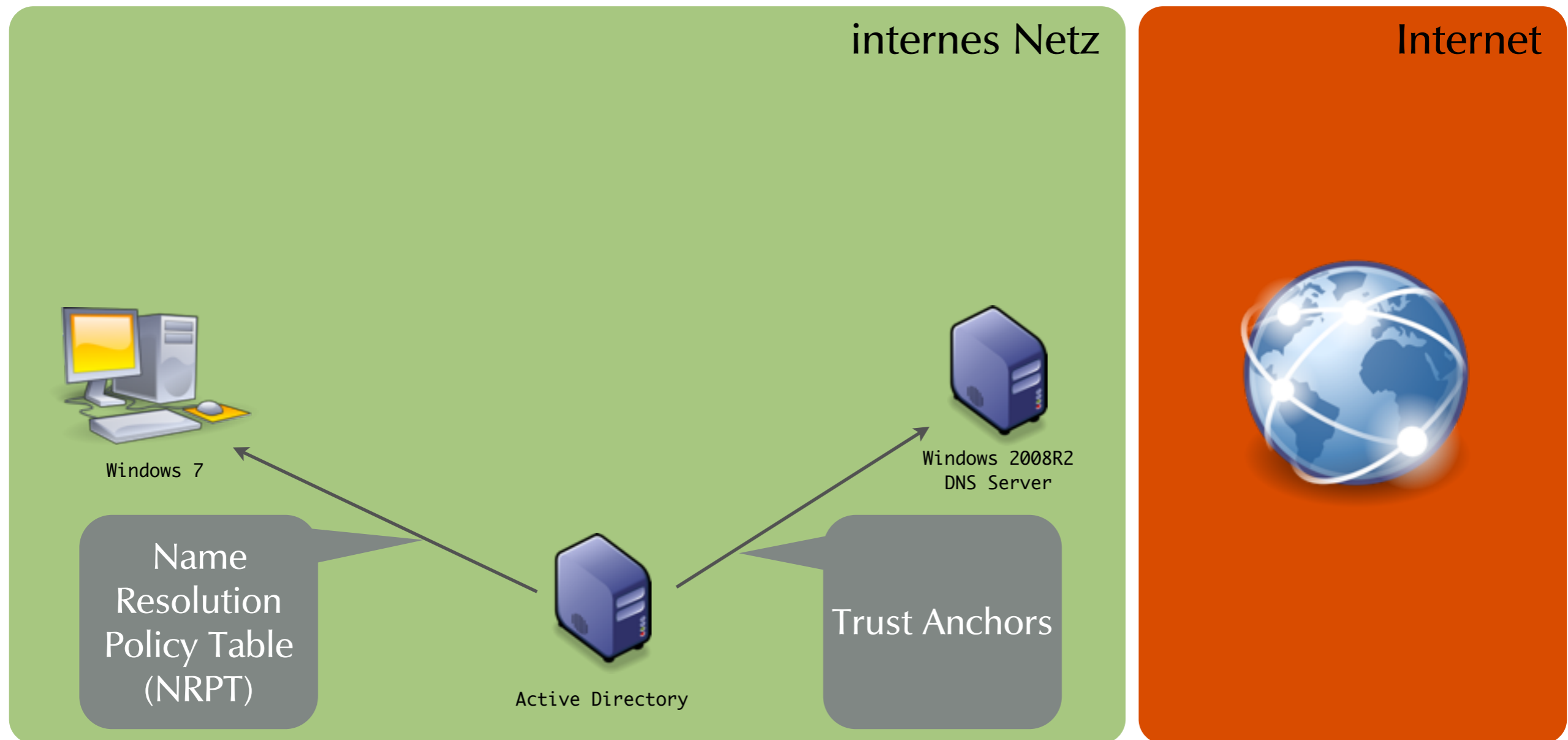
- Configure query failure options
 - Only use Link-Local Multicast Name Resolution (LLMNR) and NetBIOS if the name does not exist in DNS (most secure)
 - Always fall back to Link-Local Multicast Name Resolution (LLMNR) and NetBIOS if the name does not exist in DNS or if the DNS servers are unreachable when on a private network (moderate secure)
 - Always fall back to Link-Local Multicast Name Resolution (LLMNR) and NetBIOS for any kind of name resolution error (least secure)

Query Resolution

- Configure query resolution options
 - Resolve only IPv6 addresses for names (recommended)
 - Resolve both IPv4 and IPv6 addresses for names

OK Cancel

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

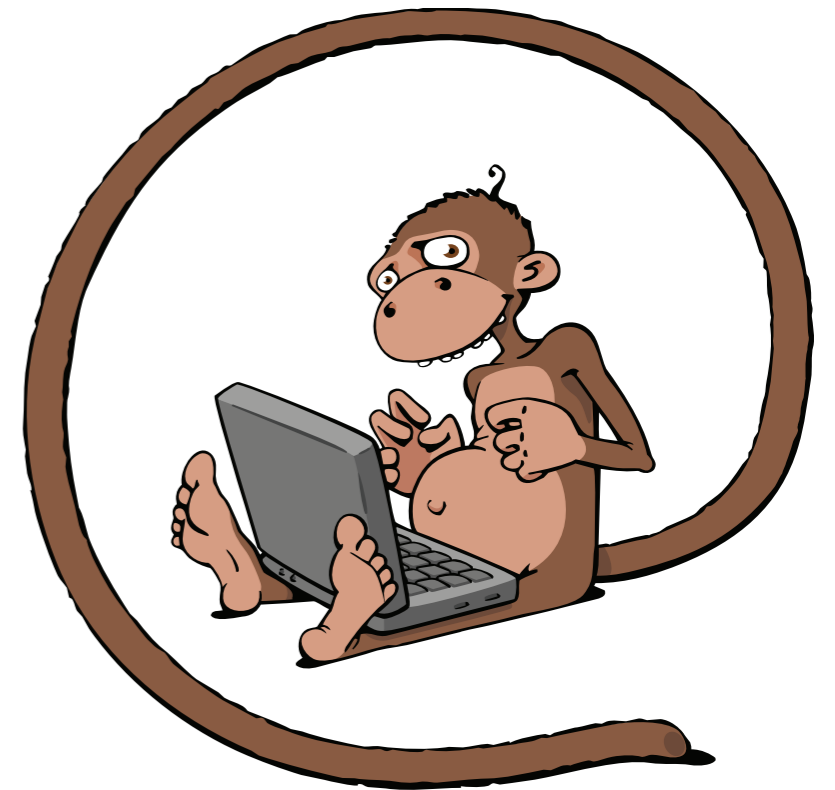
- GbDns (George Barwood DNS)
<http://www.george-barwood.pwp.blueyonder.co.uk/DnsServer/>
- geschrieben in C#, .NET
- keine externe Konfiguration (nur im Quellcode), keine GUI
- Root-Trust-Anchor einkompiliert, validiert SHA256 und NSEC3
- Recursion nur für private IP Netze (RFC 1918) + Loopback

Fragen?



MEN&MICE

© Men & Mice <http://menandmice.com>



Vielen Dank!

E-Mail:
carsten@menandmice.com

MEN&MICE

© Men & Mice <http://menandmice.com>