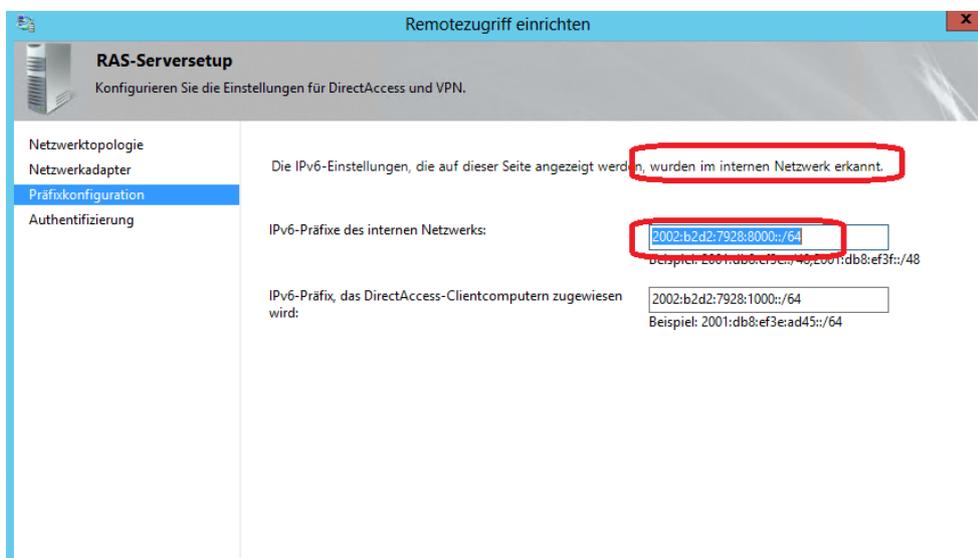


## Windows Server 2012 DirectAccess in einer bestehenden Forefront UAG DirectAccess Umgebung

Zusätzlich zu dem existierenden Forefront UAG DirectAccess Deployment wurde von mir ein neuer Windows Server 2012 DirectAccess Server mit einem Netzwerkinterface hinter einer Frontfirewall installiert welche NAT verwendet und per Portforwarding TCP443 zum Windows Server 2012 weiterleitet.

Der Kunde setzt noch flaechendeckend ISATAP ein, welches im DNS veroeffentlicht wurde und somit Netzwerkweit ein grosses /64 Bit IPv6 Subnet erstellt, welches den Forefront UAG Server als ISATAP Router verwendet.

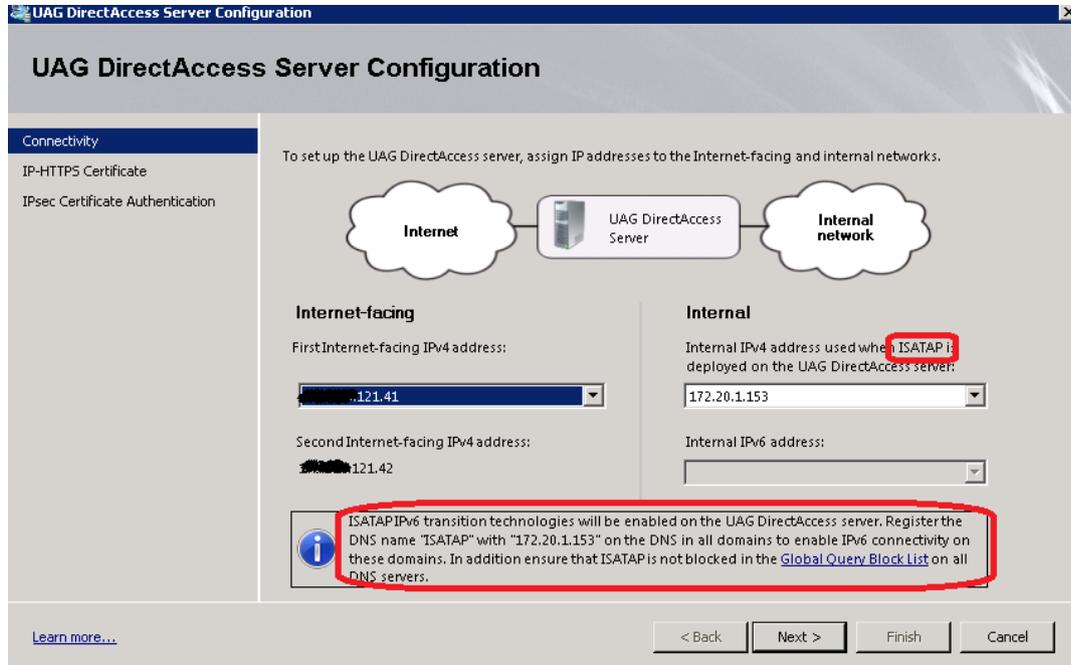
Bei der Konfiguration des DirectAccess Zugriff in Windows Server 2012 erkennt der Assistent, dass im LAN ISATAP im Einsatz ist, anhand des aktivierten ISATAP Interface auf dem Windows Server 2012 und konfiguriert DirectAccess in Windows Server 2012 zur Verwendung des ISATAP IPv6 Adressbereich.



### ISATAP Adresse des Windows Server 2012

```
Administrator: Command Prompt
Link-local IPv6 Address . . . . . : fe80::8000:::4d2d:86d6%12
Default Gateway . . . . . :
Tunnel adapter isatap.<795092EA-C84F-4205-956C-5C6062030166>:
Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2002:b2d2:7928:8000::5efe:fe80:::153%16
Link-local IPv6 Address . . . . . : fe80::5efe:fe80:::153%16
Default Gateway . . . . . :
Tunnel adapter isatap.<BDBA038C-655F-4A3D-AAAB-5F56DE842017>:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::200:5efe:fe80:::121.41%17
Link-local IPv6 Address . . . . . : fe80::200:5efe:fe80:::121.42%17
Link-local IPv6 Address . . . . . : fe80::200:5efe:fe80:::121.43%17
Default Gateway . . . . . :
Tunnel adapter IPHTTPSInterface:
Connection-specific DNS Suffix . :
IPv6 Address . . . . . : 2002:b2d2:7928:1000::e992:da26:::8c20
Link-local IPv6 Address . . . . . : fe80::e992:da26:79c8:8c20%19
Default Gateway . . . . . :
```

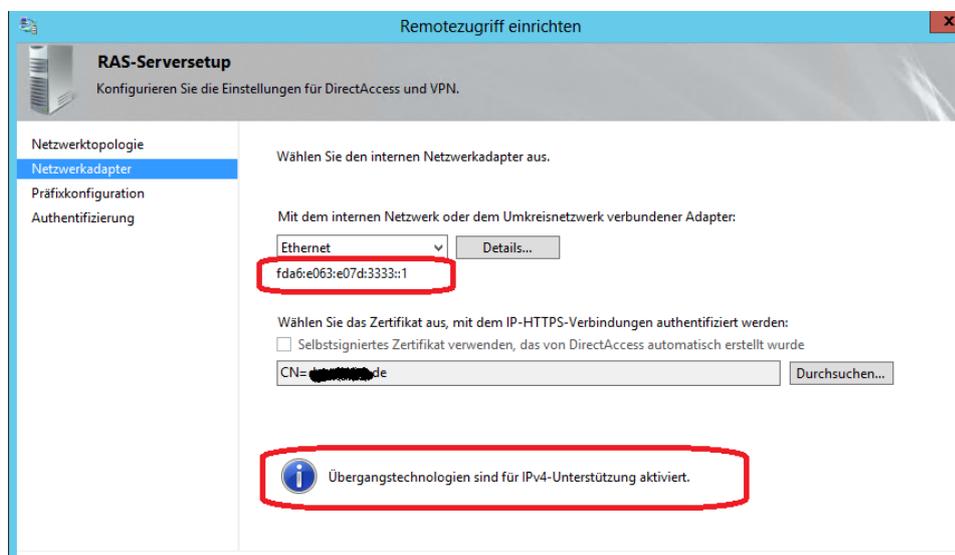
Auf dem UAG Server wird ISATAP verwendet, im DNS wurde auf allen DC das GlobalQueryBlocklist Feature deaktiviert und ein A Record fuer ISATAP erstellt welcher auf die Interne IP Adresse des UAG Servers zeigt. Somit aktiviert jeder Client ab Windows Vista SP1 und Windows Server 2008 sein ISATAP-Interface und erhaelt eine IPv6-Adresse aus dem ISATAP Router Bereich.



Der ISATAP Eintrag kann erfolgreich aufgelöst werden

```
<100% Verlust>,
C:\Users\adminmg>ping isatap
Ping wird ausgeführt für isatap.1 [172.20.1.153] mit 32 Bytes Daten:
Zeitüberschreitung der Anforderung.
Zeitüberschreitung der Anforderung.
```

Auf dem Windows Server 2012 DirectAccess Server kann man auch gut im Assistenten sehen, dass der Server fuer IPV6-Uebergangstechnologien aktiviert ist.



Somit ist der Windows Server 2012 DirectAccess Bestandteil des 64 Bit grossen IPv6 Adressraums, welcher als Standardgateway fuer IPv6 den Forefront UAG Server verwendet. Somit kommen Anfragen von DA Windows 8 Clients zum DA 2012 Server, welcher die Anfragen an die Server in dem LAN weiterleitet nicht zurueck, da die ISATAP aktivierten Infrastrukturserver alle IPv6-Antwortpakete an den Forefront UAG Server senden.

Loesung ist die dauerhafte Deaktivierung des ISATAP Interface auf dem Windows Server 2012 DA Server mit Hilfe von Netsh oder besser die globale Deaktivierung von ISATAP im LAN, was wir aufgrund der Kuerze der Zeit und der Absprache mit den Verantwortlichen nicht kurzfristig durchfuehren konnten.

```
netsh interface ipv6 isatap>
netsh interface ipv6 isatap>show state
ISATAP State           : default

netsh interface ipv6 isatap>set state disabled
Ok.

netsh interface ipv6 isatap>
```

Anschließend wurde der Windows Server 2012 DA Server einmal gebootet und der DA-Assistent nochmal neu gestartet und wie man sehen kann sind jetzt keine IPv6 Uebergangstechnologien mehr aktiv und DA 2012 funktioniert mit Windows 8 Clients problemlos.

