

# DirectAccess im Vergleich Forefront UAG vs. Windows Server 2012

**Marc Grote**

IT TRAINING GROTE

[blog.it-training-grote.de](http://blog.it-training-grote.de)

[www.it-training-grote.de](http://www.it-training-grote.de)



**\\vice:lingen**

intelligent communities for europe

# Inhalt

- Vorstellung der Rivalen
- Ueberblick ueber DirectAccess
- IPv4 / IPv6 Transitions Technologien
- DirectAccess in Forefront UAG
- DirectAccess in Windows Server 2012
- Wer hat gewonnen?
- Zukunft?

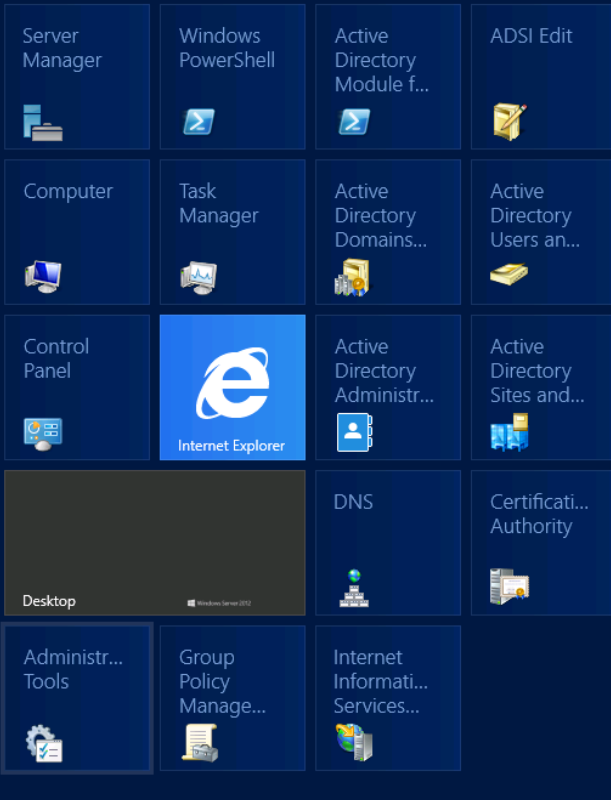
# Referentenvorstellung

Hallo, mein Name ist Marc und ich wohne  
in Deutschland (meist in Hotels)

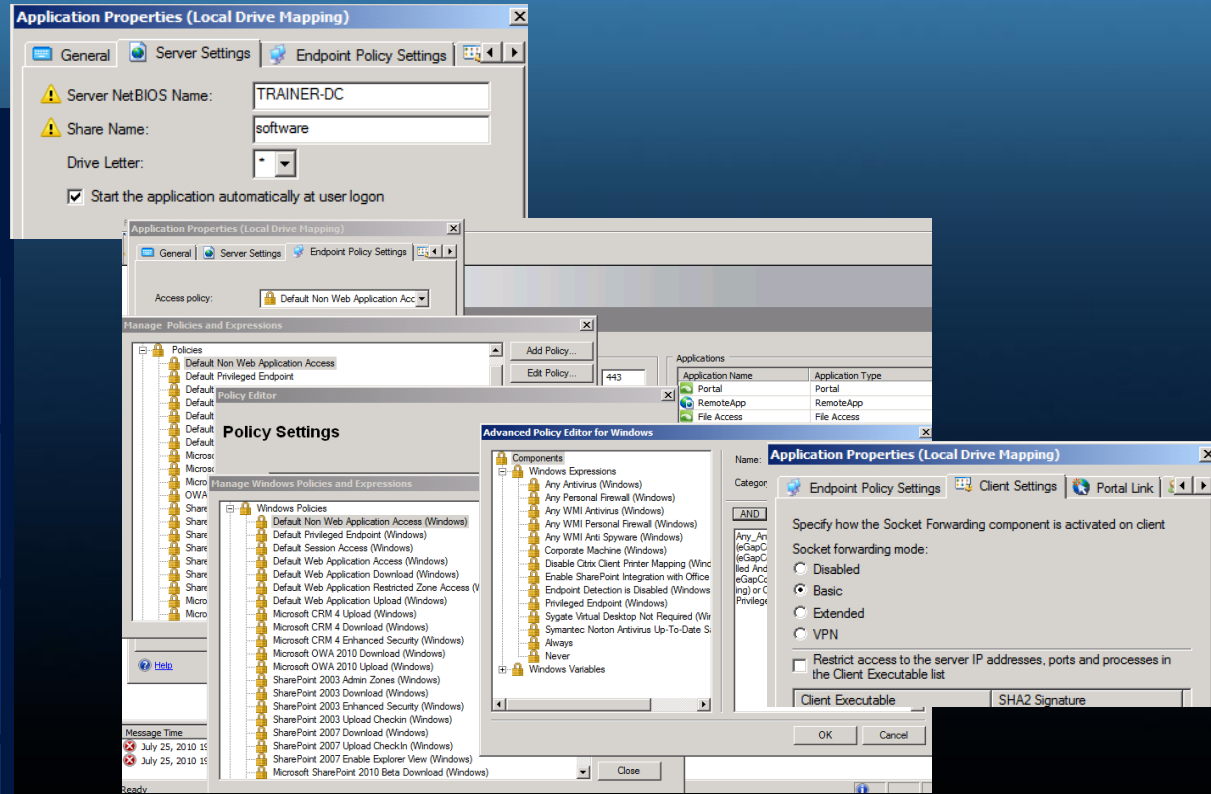


# Vorstellung der Rivalen

## Start



A grid of Windows Start menu tiles. The tiles are arranged in a 4x4 grid. The top row contains: Server Manager, Windows PowerShell, Active Directory Module f..., and ADSI Edit. The second row contains: Computer, Task Manager, Active Directory Domains..., and Active Directory Users an... The third row contains: Control Panel, Internet Explorer, Active Directory Administr..., and Active Directory Sites and... The bottom row contains: Desktop, Administr... Tools, Group Policy Policy..., and Internet Services... Each tile has a small icon representing the application or tool.



A collage of screenshots from the Windows System Management console. The main window is 'Application Properties (Local Drive Mapping)' with the 'Endpoint Policy Settings' tab selected. It shows fields for 'Server NetBIOS Name' (TRAINER-DC), 'Share Name' (software), and 'Drive Letter'. Below these are 'Access policy' and a checkbox 'Start the application automatically at user logon'. Other overlapping windows include 'Manage Policies and Expressions', 'Policy Settings', and 'Advanced Policy Editor for Windows'. The 'Advanced Policy Editor' shows a list of components with 'Windows Variables' selected. Another window shows 'Application Properties (Local Drive Mapping)' with the 'Endpoint Policy Settings' tab, displaying 'Socket forwarding mode' options: Disabled, Basic, Extended, and VPN.



# Vorstellung der Rivalen

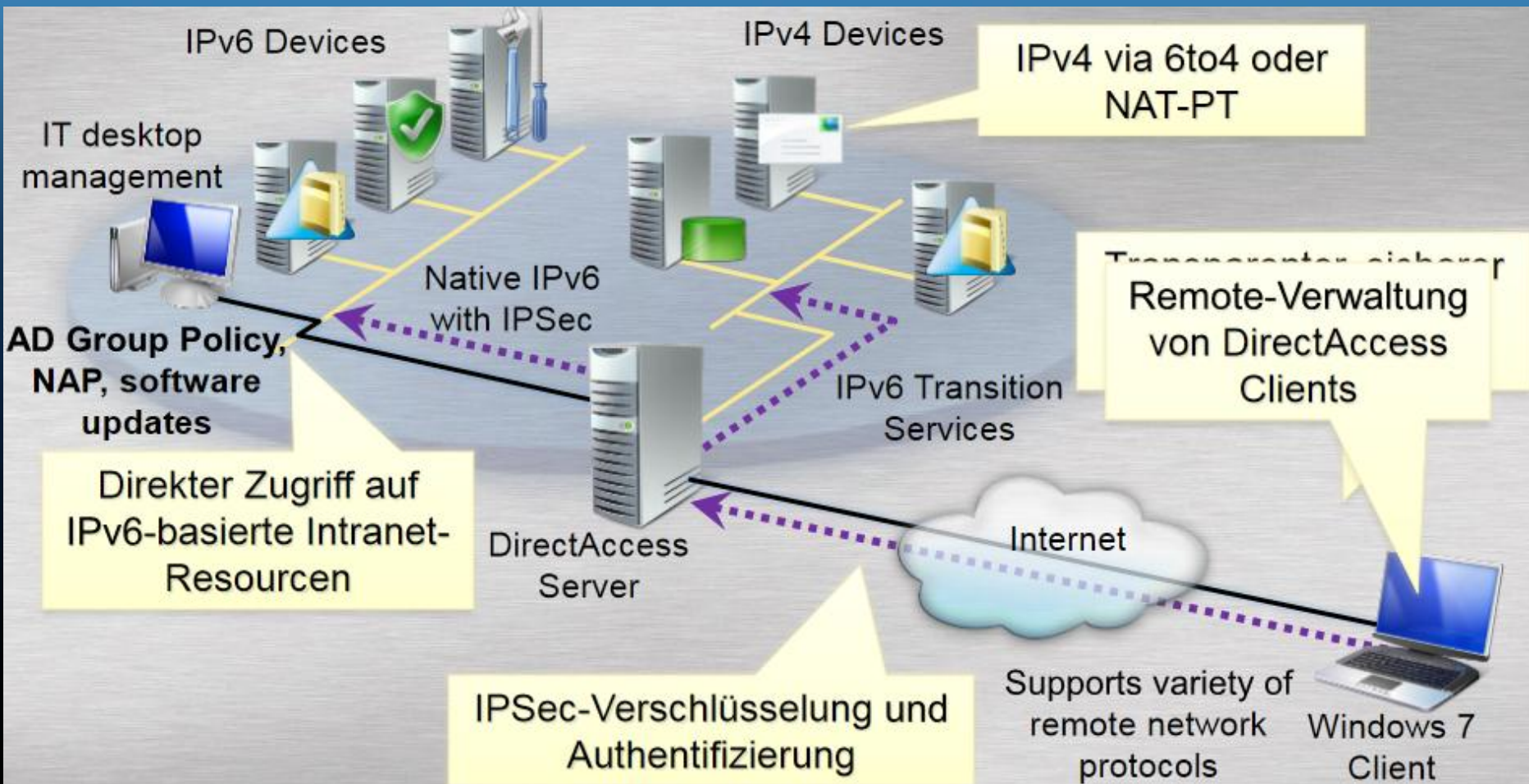
- Mehrwertdienste Forefront UAG
  - Portalloesung
  - Endpoint Access Policies
  - Erweiterter Authentifizierungssupport
  - Forefront TMG als „Personal Firewall“
  - SSL VPN fuer Windows XP mit Hilfe des UAG Network Extenders



# Demo



# Ueberblick ueber DirectAccess



# IPv4 / IPv6 Transitions Technologien

- ISATAP
  - Intrasite Automatic Tunnel Addressing Protocol. ISATAP Router gibt IPv4 Hosts IPv6 Adressen und Routing Informationen
- 6to4
  - Transitionstechnologie . DA Clients und UAG DA Server verwenden IPv6 getunnelt durch IPv4. 6to4 wird im öffentlichen IPv4 Internet verwendet. IPv6 Pakete werden in IPv4 Header gekapselt und ueber den 6to4 Tunnel Adapter zum DA Server gesendet.
- Teredo
  - Transitionstechnologie– DA Clients und UAG DA Server verwenden IPv6 ueber das IPv4 Internet. Teredo wird verwendet wenn DA Client hinter NAT Device steckt und UDP port 3544 geblockt wird. IPv6 Pakete werden in IPv4 Header gekapselt und ueber Teredo Tunnel Adapter zum DA Server gesendet.
- IP-HTTPS
  - Transitionstechnologie – DA Clients und UAG DA Server verwenden IPv6 ueber das IPv4 Internet. IP-HTTPS wird verwendet wenn der DA Client eine private IP Adresse hat, NAT verwendet wird oder die Firewall nur HTTP/HTTPS erlaubt. IPv6 wird in IPv4 gekapselt und in HTTPS verpackt
- NAT64/DNS64 – NAT64/DNS64
  - NAT64/DNS64 akzeptiert Verbindung vom DA Client, erstellt automatisch IPv6 Adressen von dem Client der vom DA Client angefragt wird und fuehrt NAT durch und leitet IPv6 Anfragen vom DA Client an das IPv4 Intranet





# DirectAccess in Forefront UAG

- Built-in NAT64 and DNS64 support for accessing IPv4-only resources
- PKI erforderlich
- CRL muss im Internet erreichbar sein
- Load Balancing Support
- Support for multiple domains
- Support for OTP (token based authentication)
- Automated support for force tunneling
- (eingeschränkter) Multisite support
- UAG Server Schutz durch Forefront TMG
- User and Health Monitoring mit UAG Webmonitor



# Demo



# DirectAccess in Windows Server 2012

- **Direct Access and RRAS coexistence**
- **Simplified Direct Access management for small and medium organization administrators**
- **Built-in NAT64 and DNS64 support for accessing IPv4-only resources**
- **Support for Direct Access server behind a NAT device**
- **Load Balancing Support**
- **Support for multiple domains**
- **Support for OTP (token based authentication)**
- **Automated support for force tunneling**
- **Multisite support**



# DirectAccess in Windows Server 2012

- **Windows PowerShell support**
- **User and Server health monitoring across all Servers**
- **Single IPSEC Tunnel im “Wizard” Mode**
- **Kerberos Proxy auf RA Server**
- **Keine Computer Zertifikate notwendig**
- **Verdoppelte PKI Performance in Server 2012**
- **IP-HTTPS Performance near Teredo Performance**
- **RSS UDP fuer DirectAccess**
- **IPSEC Hardware Acceleration in Hyper-V VM**
- **IPSEC Offload NIC unterstuetzt NIC Teaming**
- **Integrierter DCA in Windows 8**



# Demo



# Wer hat gewonnen? (auf DA bezogen)

Funktion	Forefront UAG	Windows Server 2012
SSL VPN	X (XP und hoeher)	X (Ab Vista SP1)
DirectAccess Server hinter NAT Device		X
Load Balancing	X	X
Multisite Support	X (am aufwaendigsten)	X (aufwaendig)
User and Server Health Monitoring	X (UAG Webmonitor)	X (Remote Access Konsole)
NAT64 / DNS64	X	X
PKI erforderlich	X	(bei Multisite DA ja)
Schutz des Hostsystems	X (Forefront TMG)	X (Windows Firewall)
Anzahl NIC erforderlich	2	1



Wer hat gewonnen ?



# Zukunft

- In einer reinen IPv6 Welt sind IPv4 / IPv6 Uebergangstechnologien nicht mehr notwendig
- Wie seht Ihr die Zukunft der RemoteAccess Technologie?
  - Cloud (was kommt danach)
  - Anywhere Access v2
  - ??????





# Lust auf Links

- Forefront UAG und DirectAccess  
<http://www.it-training-grote.de/download/>
- DirectAccess in Windows Server 2012 – Part I  
<http://blogs.technet.com/b/meamcs/archive/2012/05/03/windows-server-2012-direct-access-part-1-what-s-new.aspx>
- 10 Gründe gegen UAG DA  
<http://blog.concurrency.com/infrastructure/10-reasons-why-you-should-not-use-uag-for-directaccess-anymore/>
- DirectAccess in Windows Server 2012 – Part II  
<http://blogs.technet.com/b/meamcs/archive/2012/05/14/windows-server-2012-direct-access-part-2-how-to-build-a-test-lab.aspx>
- Migrate from Forefront UAG SP1 DirectAccess to Windows Server 2012  
<http://technet.microsoft.com/en-us/library/hh831658.aspx>
- IPv6 Testlab Guide  
<http://www.microsoft.com/en-us/download/details.aspx?id=10564>
- Understanding IPv6  
[http://technet.microsoft.com/en-us/library/cc786127\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc786127(v=ws.10).aspx)
- NAT64 / DNS64  
<http://technet.microsoft.com/en-us/library/ee406236.aspx>
- IPv6 Transition Technologies  
<http://technet.microsoft.com/en-us/library/bb727021.aspx>



Es gibt keine großen Entdeckungen und Fortschritte, solange es noch ein unglückliches Kind auf Erden gibt.

There 's no such thing as a discovery or progress as long as we have bitterly unhappy children on earth.

Er zijn geen grote ontdekkingen en geen vooruitgang, zolang er op deze wereld nog één kind ongelukkig is.

(Albert Einstein)



# Fragen?



# Das Ende

## Marc Grote

E-Mail: [grotem@it-training-grote.de](mailto:grotem@it-training-grote.de) (7\*16\*365)

Web: <http://www.it-training-grote.de>

Blog: <http://blog.it-training-grote.de>

XING: [https://www.xing.com/profile/Marc\\_Grote2](https://www.xing.com/profile/Marc_Grote2)

Mobile: 0176/23380279 (manchmal)

MSN: Was ist das? 😊

Twitter: Nicht mit mir

Facebook: Was bitte? -> einmal die Woche spannen und mich amuesieren was Leute so schreiben

