TRAINING-GROTE
CONSULTING&SCHULUNG

Windows Server 2012 R2 DirectAccess

Agenda

- Ueberblick ueber die DirectAccess-Technologie
- Systemvoraussetzungen
- Einrichtung einer DirectAccess-Infrastruktur
- Konfiguration von DirectAccess-Clients
- (Hoffentlich kein) Troubleshooting
- Ausblick auf weitere Moeglichkeiten
  - MultiSite DirectAccess
  - DA Hochverfuegbarkeit
  - Migration von Forefront UAG

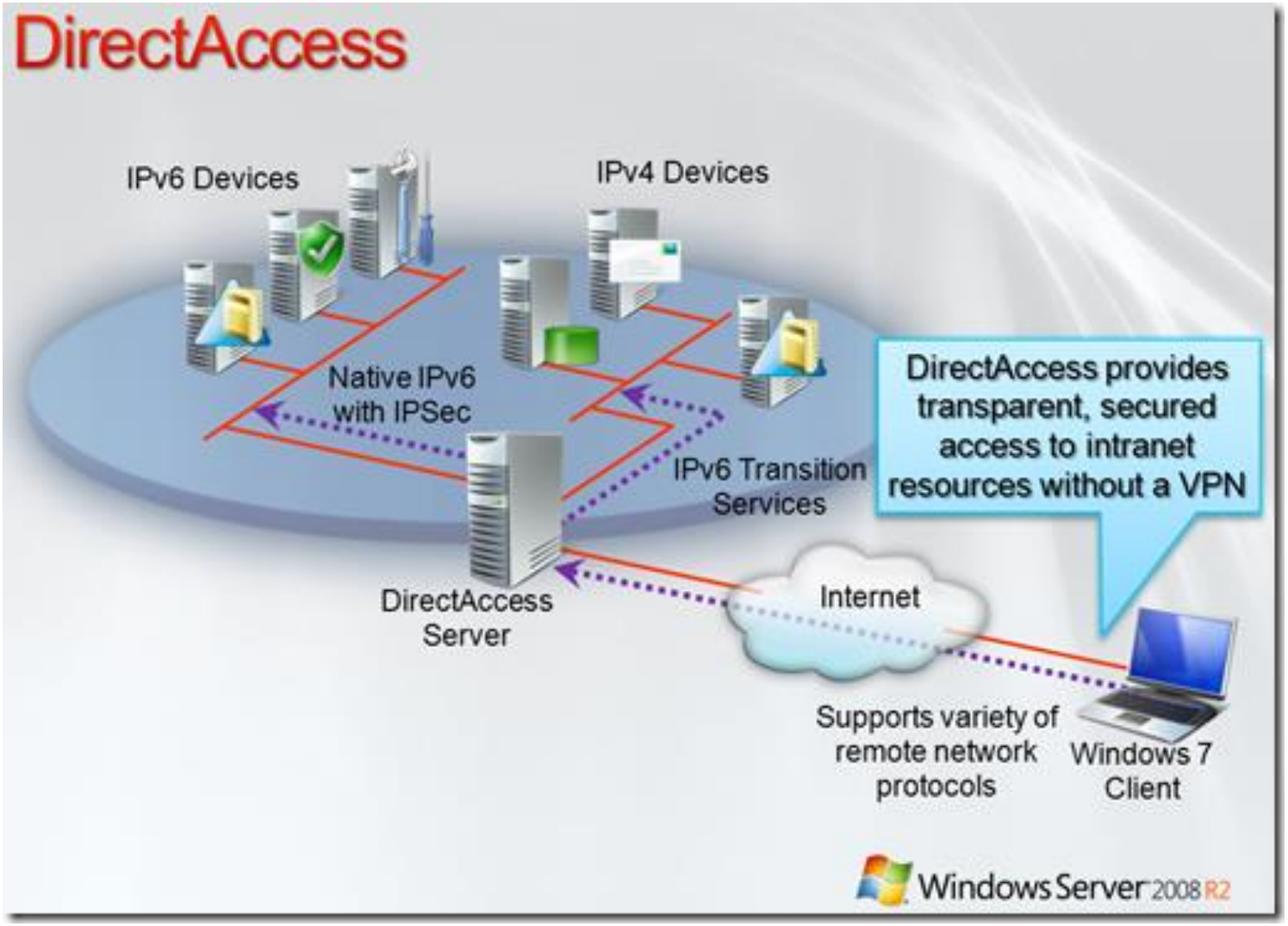
Wer bin ich?

- Marc Grote
- Seit 1989 hauptberuflich ITler / Seit 1995 Selbststaendig
- Microsoft MVP seit 2004 (2004-2014 Forefront, seit 2014 Hyper-V)
- Microsoft MCT / MCSE Messaging/Security/Server /MCLC /MCITP*/MCTS* /MCSA* /MC*
  MCSE Private Cloud
  MCS Server Virtualization Hyper-V und System Center
  MCS Implementing Microsoft Azure Infrastructure Solutions
  MCITP Virtualization Administrator
- Buchautor und Autor fuer Fachzeitschriften
- Schwerpunkte:
  - Windows Server Clustering/Virtualisierung/PKI
  - System Center DPM/SCVMM/SCEP
  - Exchange Server seit Version 5.0

DirectAccess

DA – SplitTunneling – NRPT – IPv6 – Teredo – 6to4 – IPHTTPS – Netsh – ISATAP – PKI – NAP – OTP – KerbProxy – NLS – NLB – HLB – RRAS – Edge – NAT – NAT-T – GPO – ForceTunnel – NCA – DCA – DNS Suffix – DNS Suffix Search List – NAT64 – DNS64 – Kerberos – NTLM – Management Server – RADIUS – Computer Zertifikate – EKU - Accounting – Inbox Accounting – URA – VPN – SSTP – NPS – EntryPoint – CRL – CDP - AIA

DirectAccess im Ueberblick



Quelle: http://blogs.technet.com/b/aviraj/archive/2009/10/09/directaccess-design-guide-for-windows-7-and-windows-server-2008-r2.aspx

IPv4 / IPv6 Transitions Technologien

- ISATAP

  Intrasite Automatic Tunnel Addressing Protocol. ISATAP Router gibt IPv4 Hosts IPv6 Adressen und Routing Informationen

- 6to4

  Transitionstechnoloie . DA Clients und DA Server verwenden IPv6 getunnelt durch IPv4. 6to4 wird im oeffentlichen IPv4 Internet verwendet. IPv6 Pakete werden in IPv4 Header gekapselt und ueber den 6to4 Tunnel Adapter zum DA Server gesendet.

- Teredo

  Transitionstechnoloie– DA Clients und 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 DA Server verwenden IPv6 ueber das IPv4 Internet. IP-HTTPS wird verwendet wenn der DA Server 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 Windows Server 2012 R2

- Direct Access und RRAS Koexistenz
- Vereinfachte Direct Access Verwaltung fuer kleine und mittlere Umgebungen
- Built-in NAT64 und DNS64 Support fuer IPv4-Clients
- Support fuer Direct Access Server hinter einem NAT-Geraet
- Load Balancing Support
- Support for OTP (Token basierte Authentifizierung)
- Unterstuetzung fuer Force Tunneling
- Multisite Support
- Windows PowerShell Support

DirectAccess in Windows Server 2012 R2

- Benutzer und Server Health Monitoring fuer alle Server
- Single IPSEC Tunnel im “Wizard” Mode
- Kerberos Proxy auf DA-Server
- Keine Computer Zertifikate notwendig
- Verdoppelte PKI Performance in Server 2012 R2
- IP-HTTPS Performance nahe Teredo Performance
- Integrierter DCA in Windows 8 / 8.1

DirectAccess Systemvoraussetzungen

- http://technet.microsoft.com/en-s/library/jj574101.aspx
- Sizing beachten
- Verwendete Firewall Topologie
- Multisite erforderlich?
- Hohe Verfuegbarkeit erforderlich?
- Windows 7 Clients im Einsatz?
- IPv6 im CorpLAN im Einsatz?

Einrichtung einer DirectAccess-Infrastruktur

- Windows Server 2012 R2 als DirectAccess Server
- DA Server mit 1 oder 2 Netzwerkkarten
- DA Server hinter Firewall mit / ohne NAT
- DA Server direkt am Edge (vermeiden?!)
- Unterstuetzte Windows Clients
- PKI (optional bei Easy und nur Windows 8.x Clients)
- NLS Server auf DA Server separat (auf DA Server bei Easy)
- Active Directory / Gruppenrichtlinien

DA Geschmacksrichtungen

- Alles easy oder ….
- Advanced!

DA ist easy

- Windows Firewall must be enabled on all profiles
- Only supported for clients running Windows 8/8.1 Enterprise
- ISATAP in the corporate network is not supported
- A public key infrastructure is not required (Siehe GPO Umbiegungen)
- Not supported for deploying two-factor authentication. Domain credentials are required for authentication
- Automatically deploys DirectAccess to all mobile computers in the domain (Achtung!)
- Traffic to the Internet does not go through DirectAccess. Force tunnel configuration is not supported
- DirectAccess server is the network location server
- Network Access Protection (NAP) is not supported
- Changing policies by using a feature other than the DirectAccess management console or Windows PowerShell cmdlets is not supported

DA Advanced

- A public key infrastructure must be deployed
- Windows Firewall must be enabled on all profiles
- ISATAP in the corporate network is not supported. If you are using ISATAP, you should remove it and use native IPv6
- Computers that are running the following operating systems are supported as DirectAccess clients:
  Windows Server 2012 /R2
  Windows 8 / 8.1 Enterprise
  Windows Server 2008 R2
  Windows 7 Ultimate / Enterprise
- Force tunnel configuration is not supported with KerbProxy authentication
- Changing policies by using a feature other than the DirectAccess management console or Windows PowerShell cmdlets is not supported
- Separating NAT64/DNS64 and IPHTTPS server roles is not supported
- Multisite Support
- HA Support

DA Advanced - Infrastruktur

- WS2012-DC - DC
- TMG-EN - Firewall
- SQL2012R2 - SQL DB fuer SC
- SCOM2012 - SCOM
- SCEP2012 - SCCM
- W8-CL4-DE - DA Client
- WS2012-DA - DA
- WS2012-RDS1 - NLS

DA Advanced

Demo

DirectAccess Einrichtung (EASY)

Infrastruktur vorbereiten

DA Server vorbereiten

DA Installation / Konfiguration

DA Client aktivieren

Funktionen testen

Troubleshooting

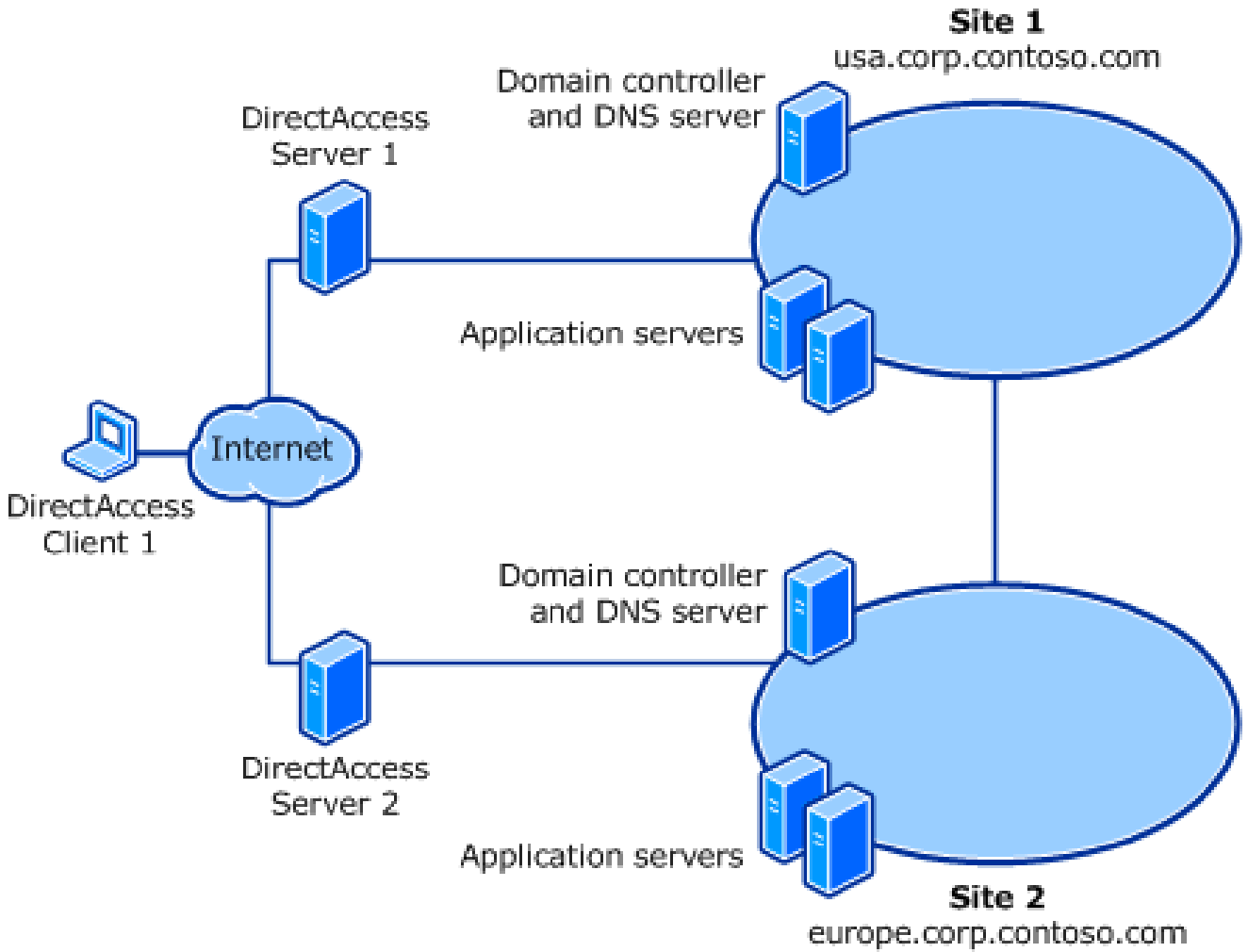
DirectAccess Einrichtung (EASY)

Demo

DirectAccess Troubleshooting

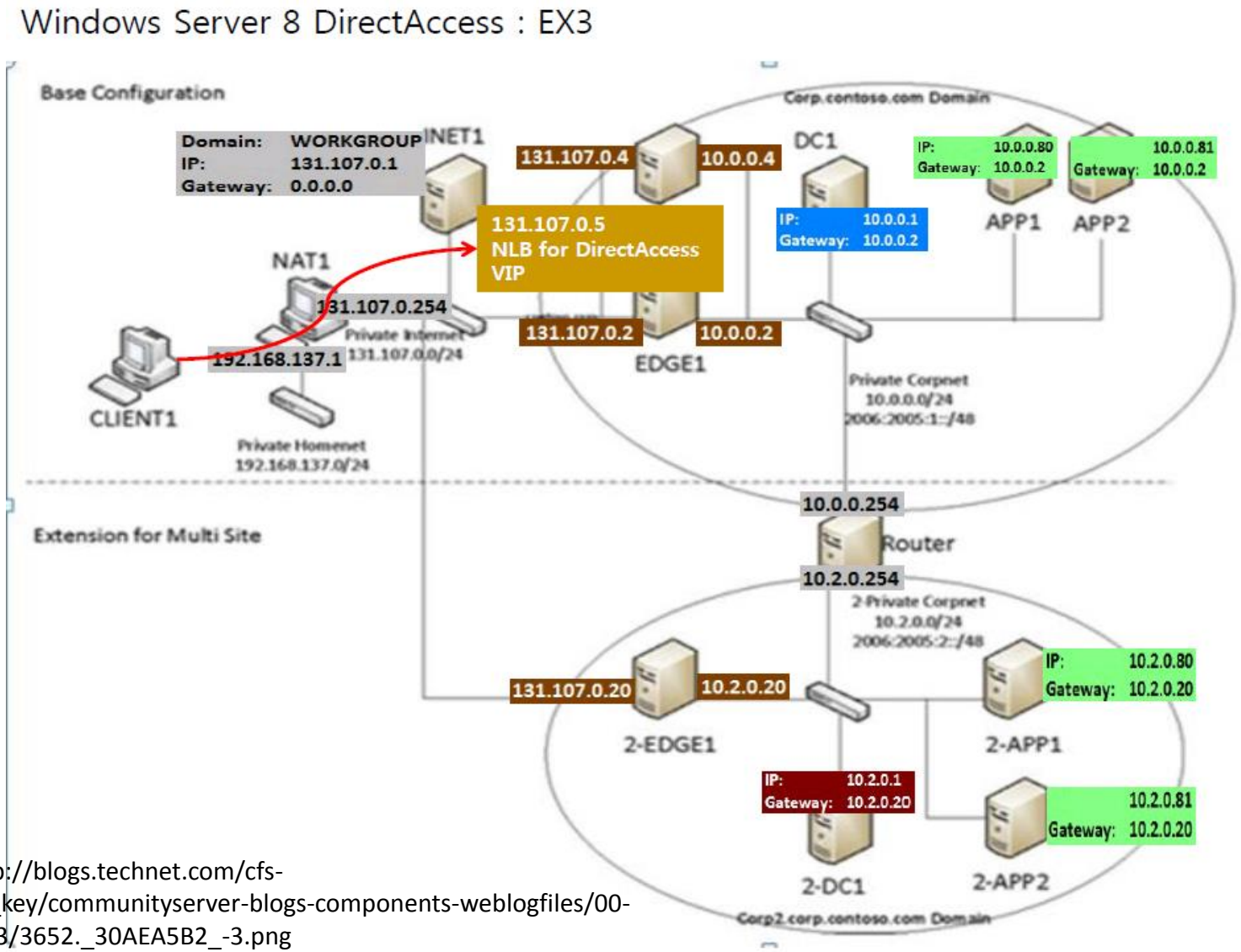
- URA Konsole
- Windows Event Viewer
- Netsh / Netsh / Netsh /Netsh
- CAPI Logging
- DCA / NCA auf Client Seite

Multisite DirectAccess



Quelle: http://i.technet.microsoft.com/dynimg/IC396155.gif

DirectAccess Hochverfuegbarkeit



Quelle: http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-85-33/3652._30AEA5B2_-3.png


Fragen?

Kontakt

Marc Grote

- E-Mail: grotem@it-training-grote.de
- Web: http://www.it-training-grote.de
- Blog: http://blog.it-training-grote.de
- XING: https://www.xing.com/profile/Marc_Grote2
- Mobile: 0176/23380279