Campus Days
14.-16. januar 2010

# DirectAccess med Windows 7 og Windows Server 2008 R2

Jens Ole Kragh

JensOle.Kragh@eg.dk

EG A/S

Microsoft TechNet

# Jens Ole Kragh: Hvem er jeg?

- Senior Infrastruktur Arkitekt i EG A/S
  - MCITP: Server og Enterprise Administrator
  - MCITP: Windows 7, Enterprise Desktop Administrator
  - MCTS: Configuration Manager, Virtualization
  - Microsoft Certified Trainer
  - TechNet Influent Denmark
- Blogs:
  - http://jensolekragh.spaces.live.com
  - http://scug.dk og http://it-experts.dk/blogs/jok/

# Sessionens formål

- Præsentere DirectAccess
- Forklare DirectAccess teknologier
- Gennemgå muligheder og krav
- 1. step, når man vil igang med DirectAccess

# Agenda

- Behov - Ekstern adgang
- DirectAccess – Hvad er det/Hvad kan det ?
- DEMO – DirectAccess set fra en Windows 7 klient
- DirectAccess – Teknisk gennemgang
- DEMO – DirectAccess simpel konfiguration
- Hvordan kommer man i gang?
- Q and A

**Behov:**

***Ekstern adgang***

# Behov

## Mobile & fjern brugerere:

- Kunne arbejde alle steder fra
- Hurtig forbindelse
- Samme brugeroplevelse både internt og eksternt

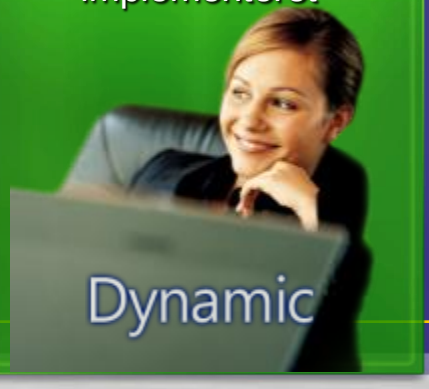
## IT afdelingen:

- Sikker og flexibel infrastruktur for “work anywhere”
- Let administration af brugere og pc’er
- Reducere omkostninger

# Network Access Infrastructure Optimization Model

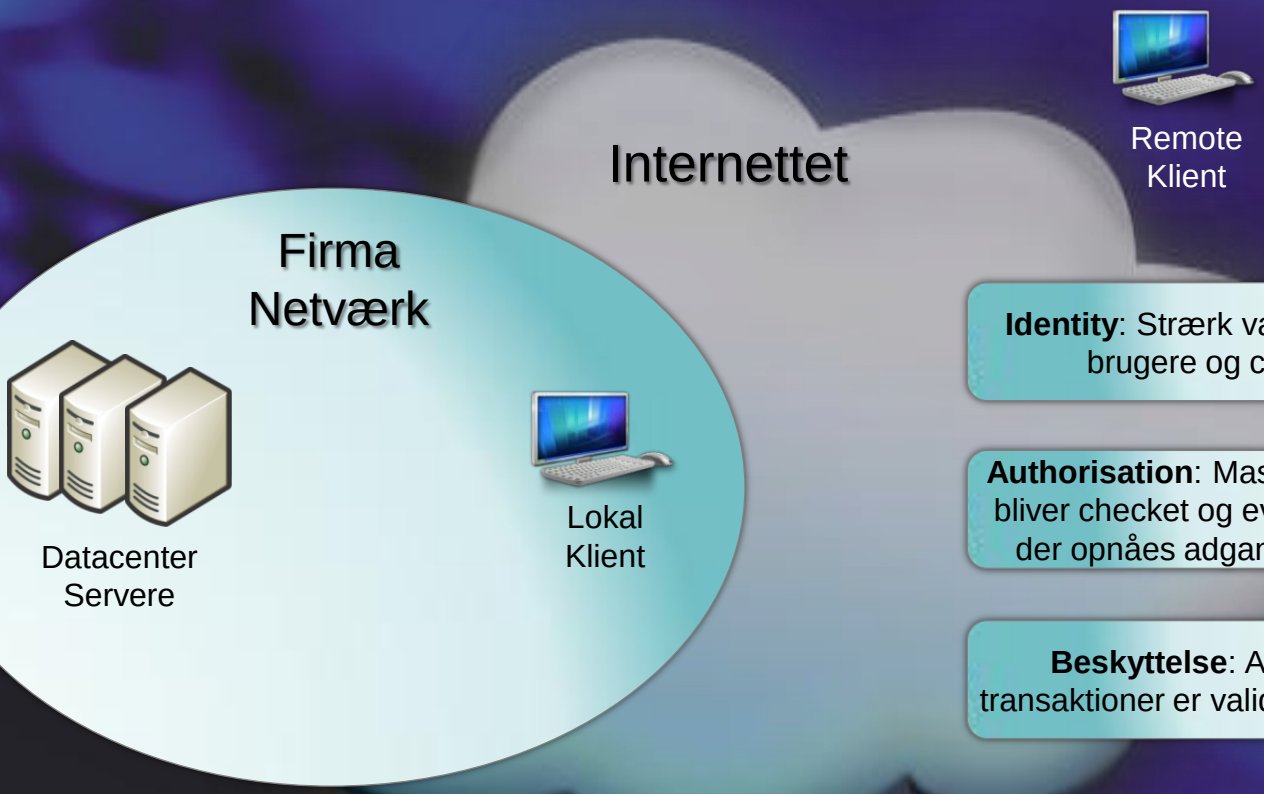
## Er IT et kostcenter eller et strategisk værktøj?

| Kost Center | Mere effektivt Kost Center | Business Enabler | Strategisk værktøj |
|---|---|---|---|
| Ingen password policies | Stærk password policy | Stærk password policy | Stærk validering |
| Kun perimeter firewalls | Host-baserede firewalls | Basis IPsec policies | Netwærks transaktioner er valideret, måske krypteret |
| Antivirus er ikke nødvendig eller ikke installeret default | Sikkerheds suite installeret på klienter | Health policies er i brug | Policy-baseret netværk tilgang med auto-remediation |
| Ingen Remote Access policies | Remote Access er tilgængelig | Remote brugeroplevelse er ens med den lokale | Remote brugere er en udvidelse af firmanetværket |
| Kun IPv4 netværk | IPv6 planlægning og test er igang | IPv6 blokeringer fjernet, addresserings plan færdig | IPv6 er fuldt implementeret |
| Basic | Standardized | Rationalized | Dynamic |



Microsoft TechNet

# Trustworthy - Netværks vision




**Identity**: Strærk validering for alle brugere og computere

**Authorisation**: Maskinens "helbred" bliver checket og evt. opdateret, før der opnåes adgang til netværket

**Beskyttelse**: Alle netværks transaktioner er valideret og krypteret

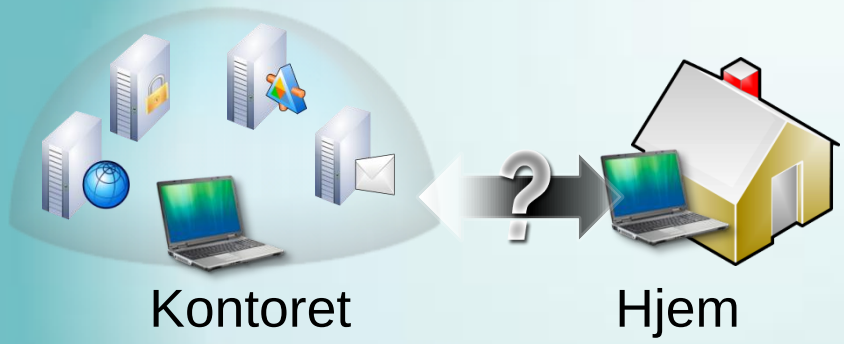
*Politikker er baseret på identiteter,*
*ikke på lokation eller hvor man befinder sig!*

# DirectAccess

## *Hvad er det og hvad kan det ?*

# Fjernadgang for mobile brugere

## Situationen i dag




- Udfordring for IT afdelingen at administrere og opdatere mobile Pc'er når der er “disconnected” fra firma netværket
- Besværligt for brugerne at tilgå firma ressourcer, når de ikke er på firma netværket
- Afhængig af leverandør af firewallen (VPN)

## Windows 7 løsning

**DirectAccess**


- Firma netværket inkluderer domain-joined klienter, lige meget hvor de er på internettet
- Nemt at administrere mobile pc’er (opdateringer, policies, software osv.)
- Øger produktiviteten: Tilbyder samme oplevelse for brugeren, internt og eksternt

# DirectAccess er:

*En sikker udvidelse af netværket og valgte netværks services*
*til virksomhedens fjern brugere*

# DirectAccess

## *- en fantastisk teknologi*

### *Altid Online*

Forbedret produktivitet

Ikke initieret af brugeren

Simpel forbindelse

### *Let admini-stration*

"Manage" remote klienter

Øger patch hit rates og management

Remote maskiner får kørt GPOs på

### *Access politikker*

Pre-logon helbreds check og remediation

Erstatter "health" check ved logon

Fuld NAP integration

### *Beskyttede transaktioner*

Supporter validerede transaktioner

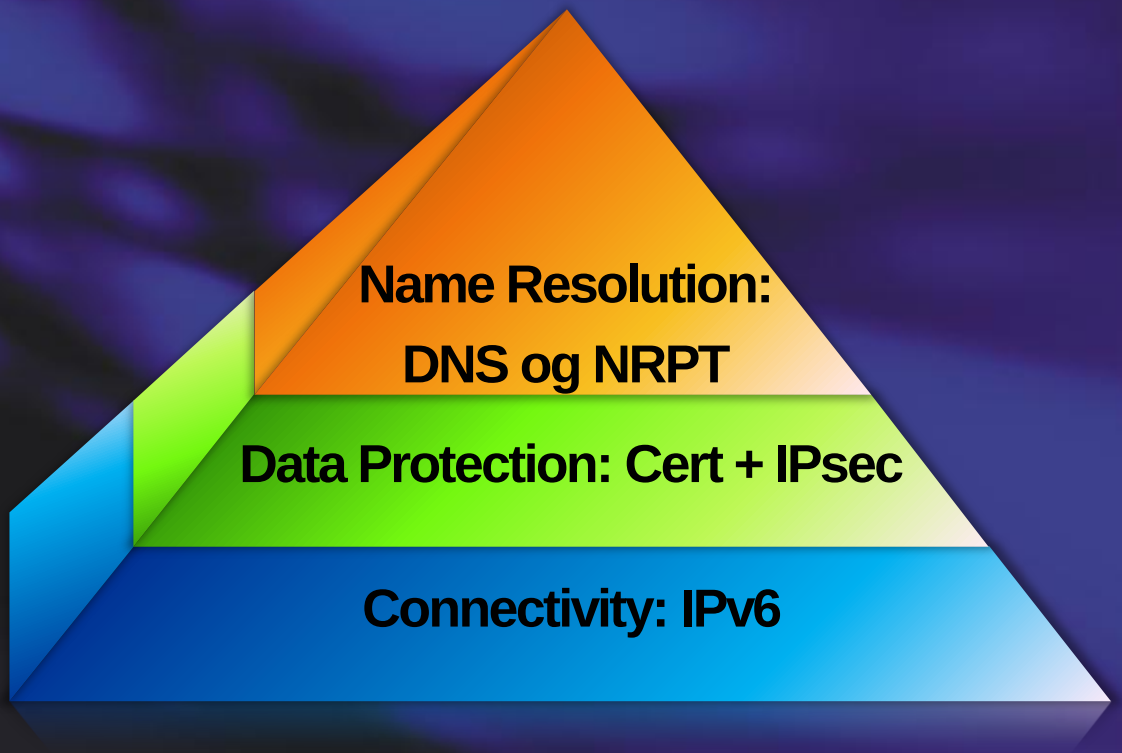
Supporterer krypterede transaktioner

Validering og kryptering forhindrer mange attacks

*VPNs forbinder brugeren til netværket*
*DirectAccess udvider netværket til brugeren*

# DirectAccess

## Teknisk fundament



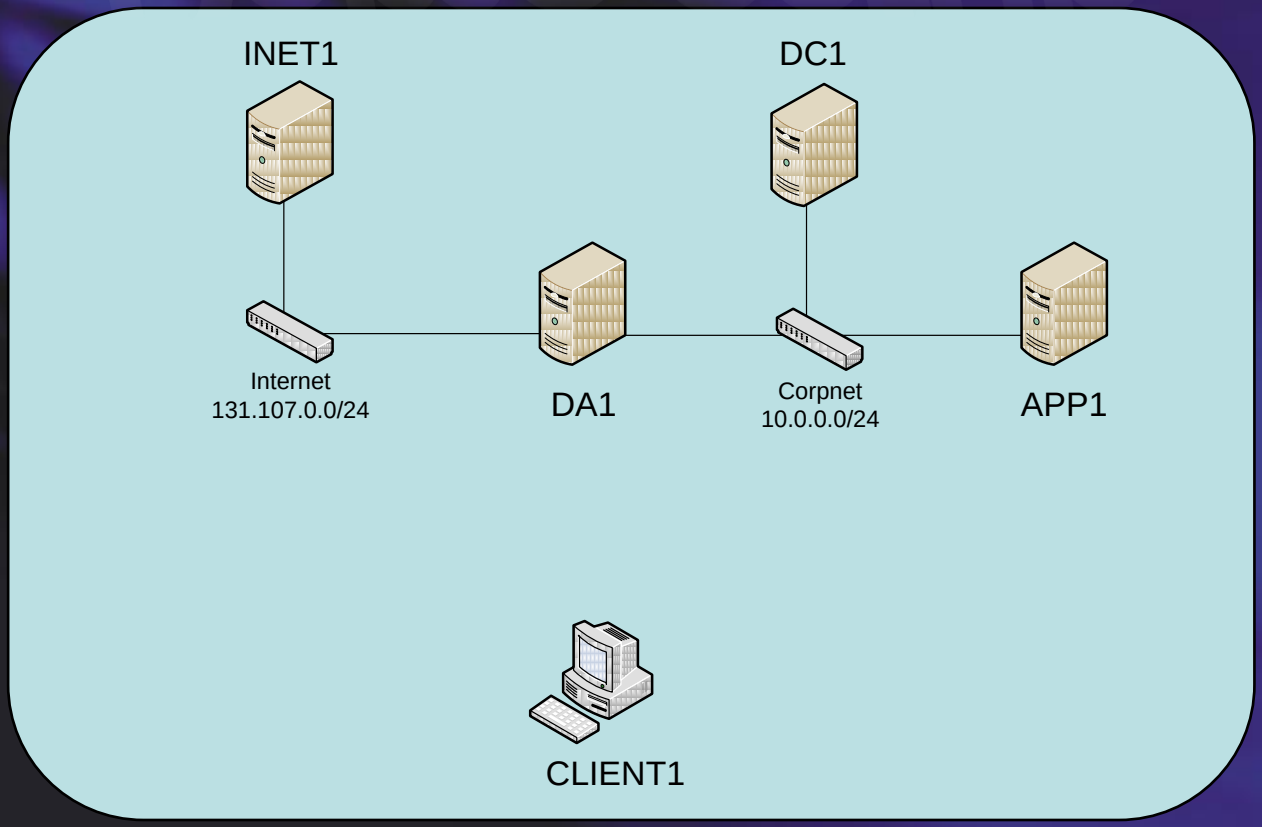
# Forbindelses processen

1. Netværk detection
2. Check intranet Web site
3. Forbinder til DirectAccess server (IPv6, 6to4, teredo, IP-HTTPS)
4. Validering med Computer Certifikat
5. Validering gruppemedlemskab
6. Helbredscheck (NAP)
7. DirectAcces forbindelsen er oppe!


# DirectAccess

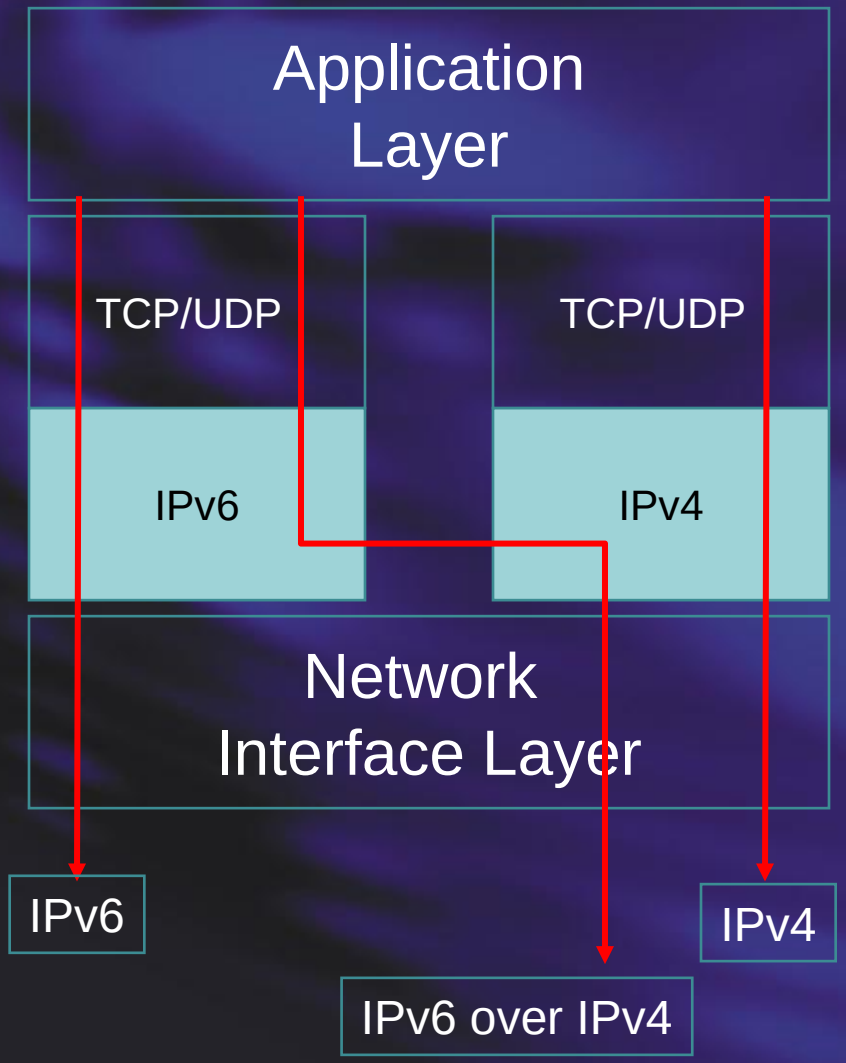
Set fra en Windows 7 klient

# Demo setup

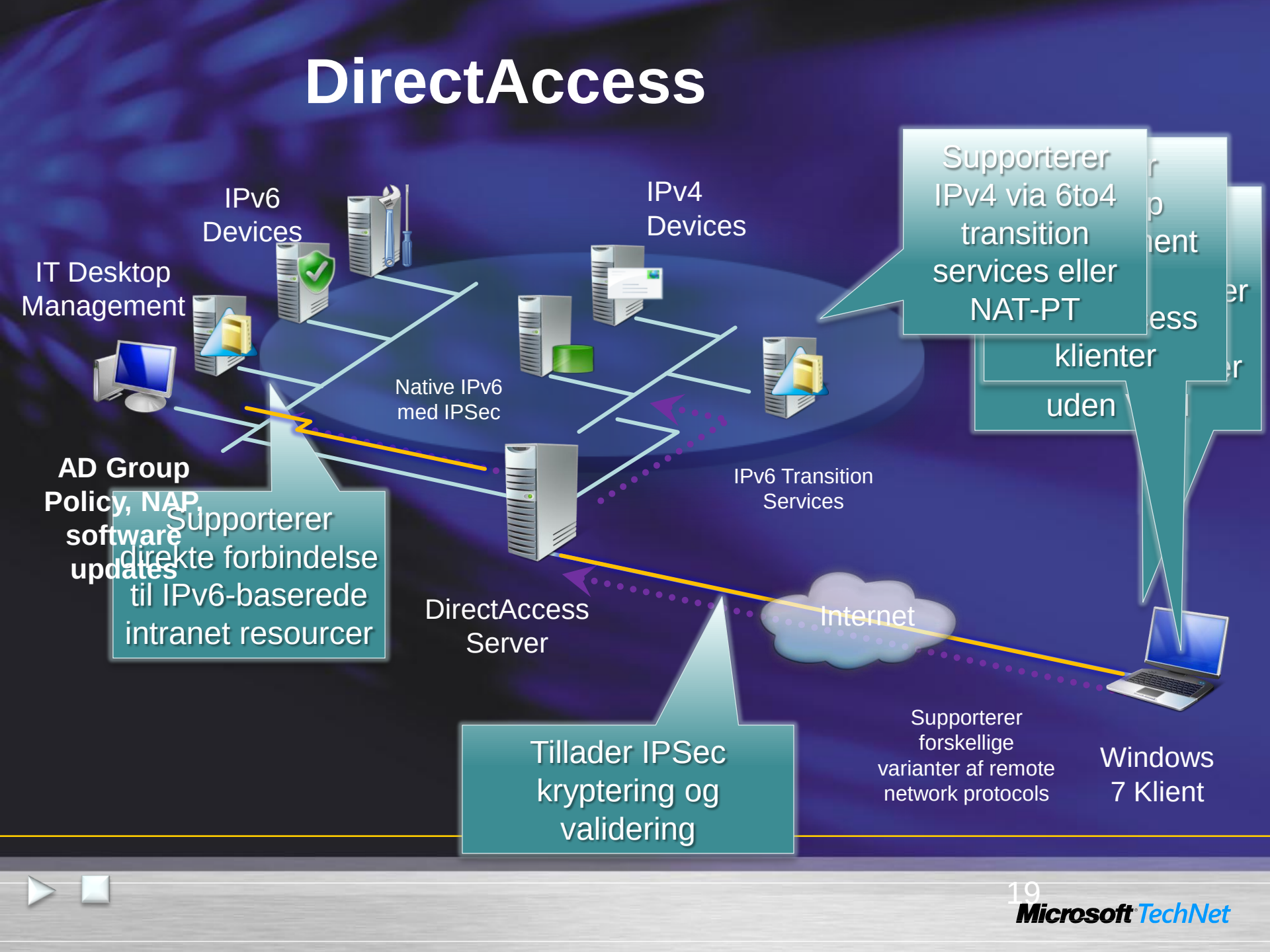

INET1
DC1
Internet
131.107.0.0/24
DA1
Corpnet
10.0.0.0/24
APP1
CLIENT1

# DirectAccess
# Teknisk gennemgang

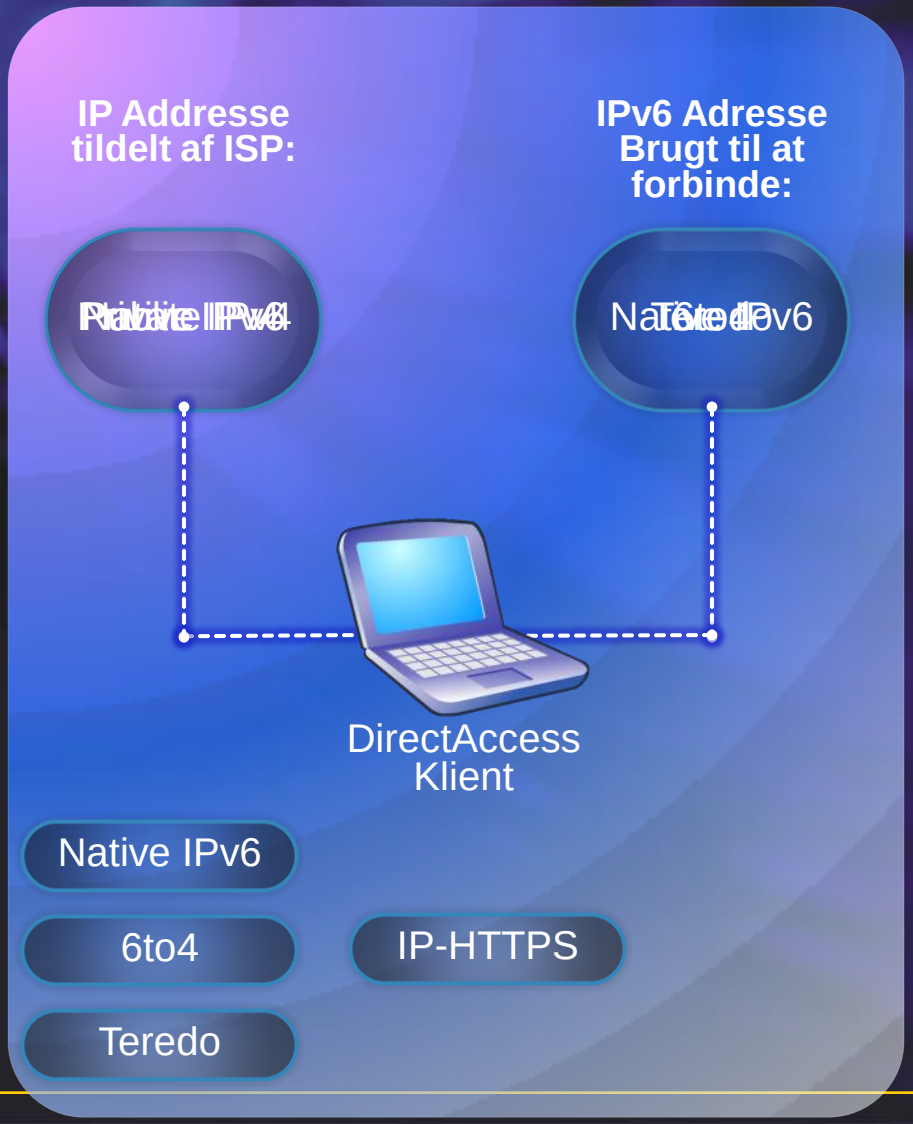
# Protokoller: IPv6, IPv4 og 6to4



# DirectAccess



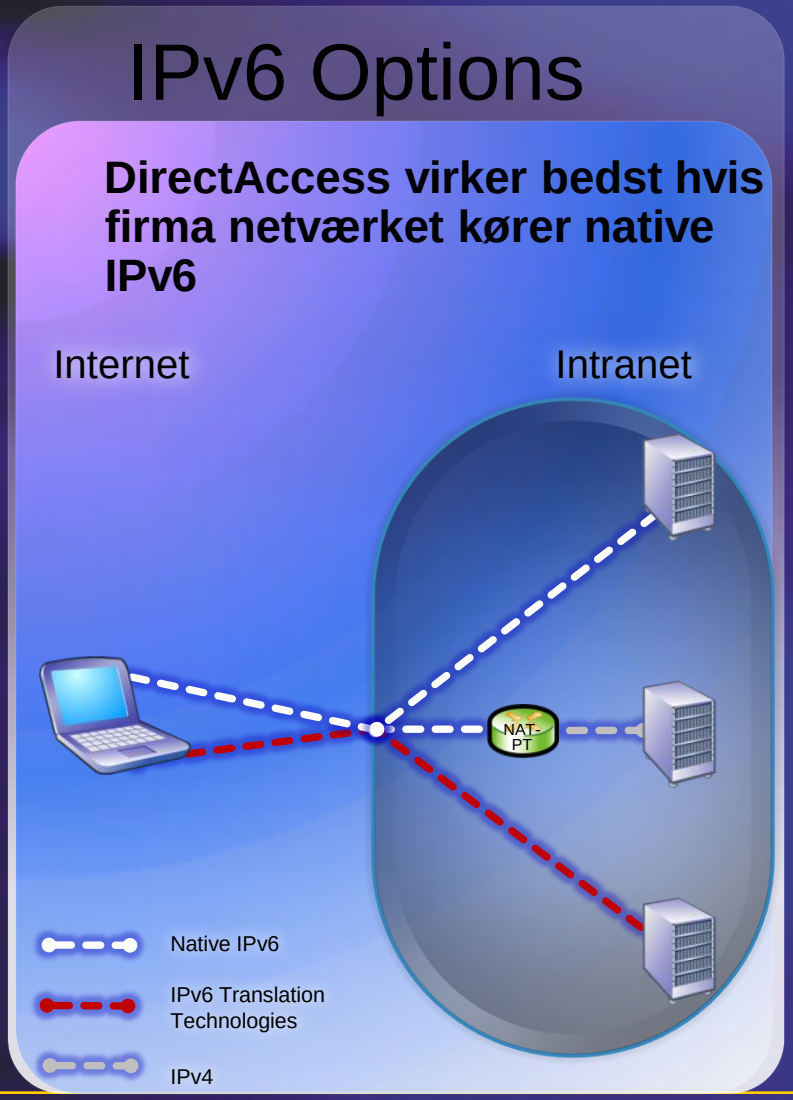
# Forbindelsen fra internettet




- Native IPv6 support
- Offentlige IPv4 adresser bruger 6to4 for at indeholde IPv6 inden i en IP Protocol 41
- Private IPv4 adresser bruger Teredo for at indeholde IPv6 inden i en IPv4 UDP (UDP 3544)
- Hvis en klient ikke kan forbinde til DirectAccess Serveren, så anvendes IP-HTTPS til at forbinde over port 443

# IPv6 Internt

- **Native**
  - Serverene kan køre hvilket som helst OS der fuldt supporterer IPv6
  - kræver IPv6 infrastruktur
  - Bedste valg
- **ISATAP**
  - IPv6 inden i IPv4
  - Serverne skal være Windows Server 2008 eller R2
  - Ingen routere skal opgraderes
- **NAT-PT**
  - "Oversætter" IPv6 til IPv4
  - virker med alle OS
  - UAG har NAT-PT "built in"



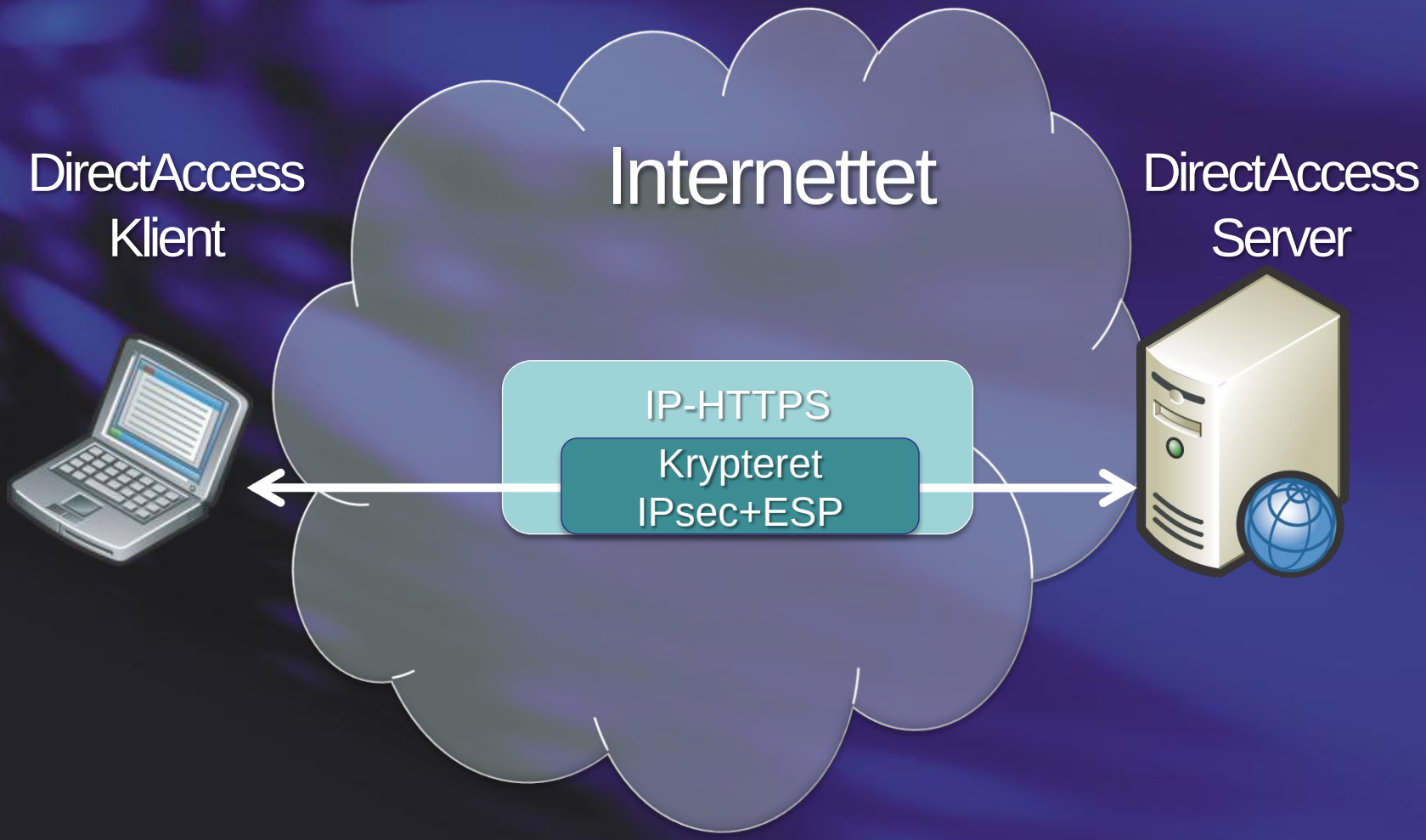
# DirectAccess

## *IPsec Data Protection*

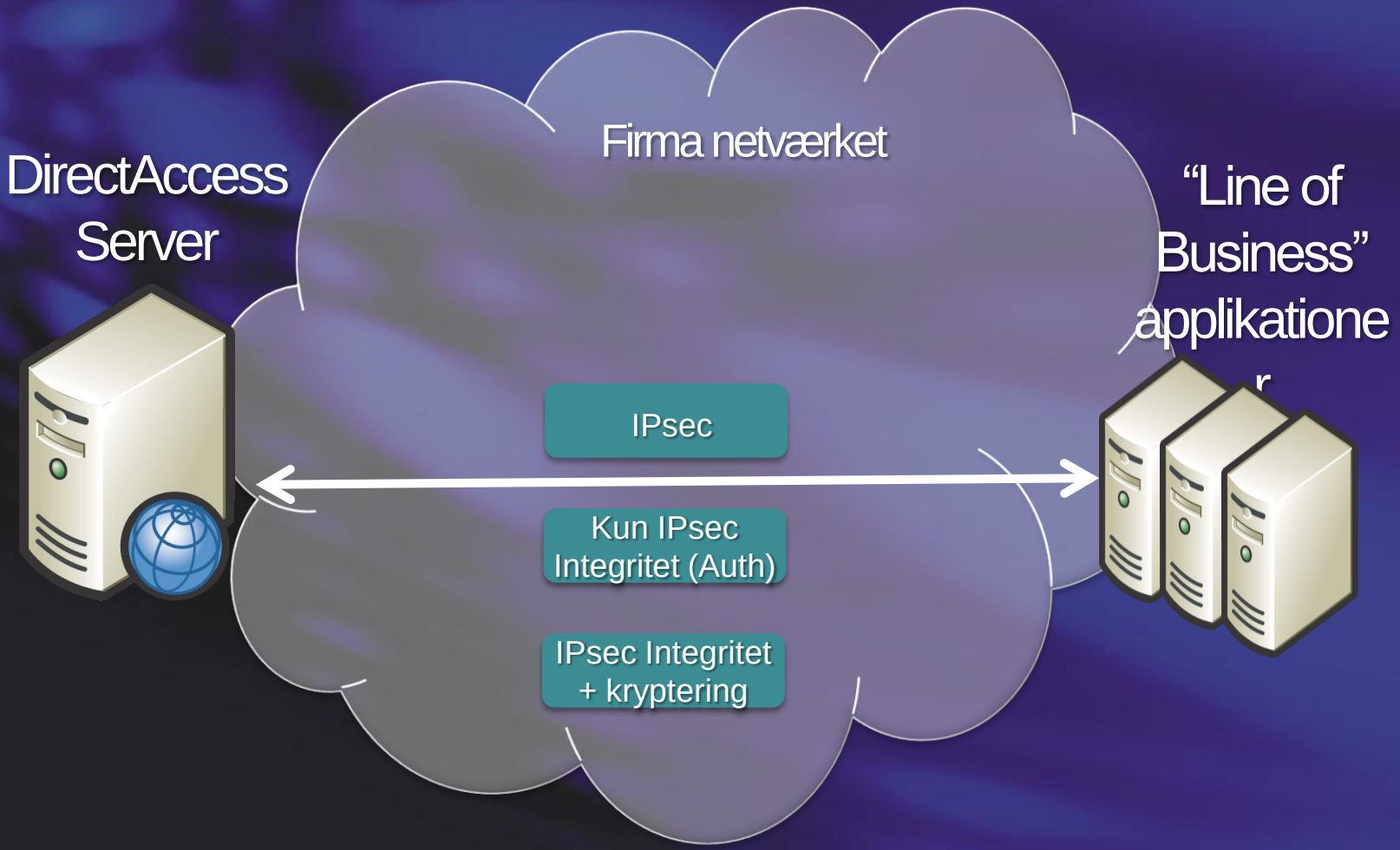

Kryptering
- End to edge
- End to end

Authentication
- End to edge
- End to end

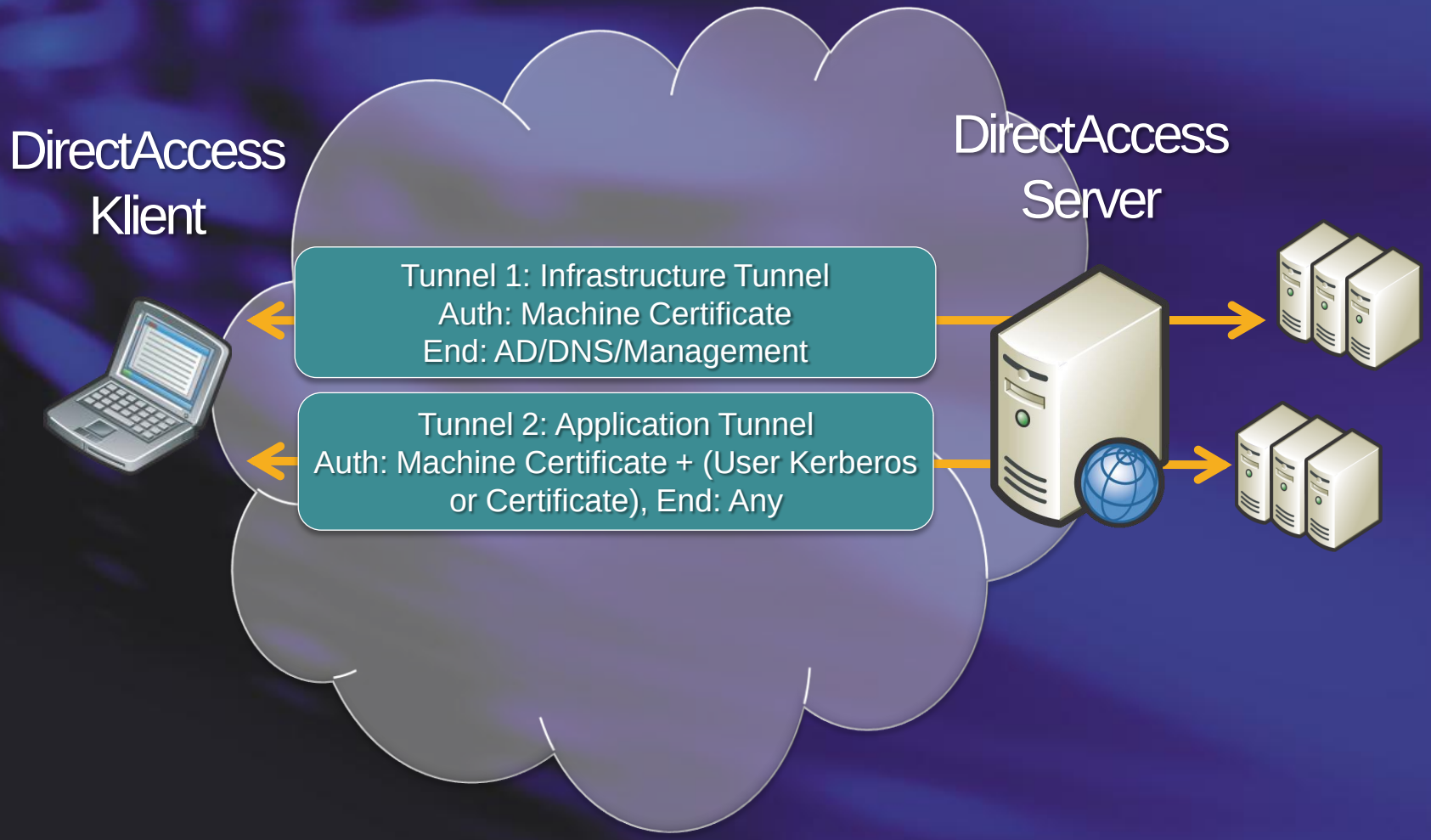
# IPsec eksternt



# IPsec internt



# IPsec tunnel

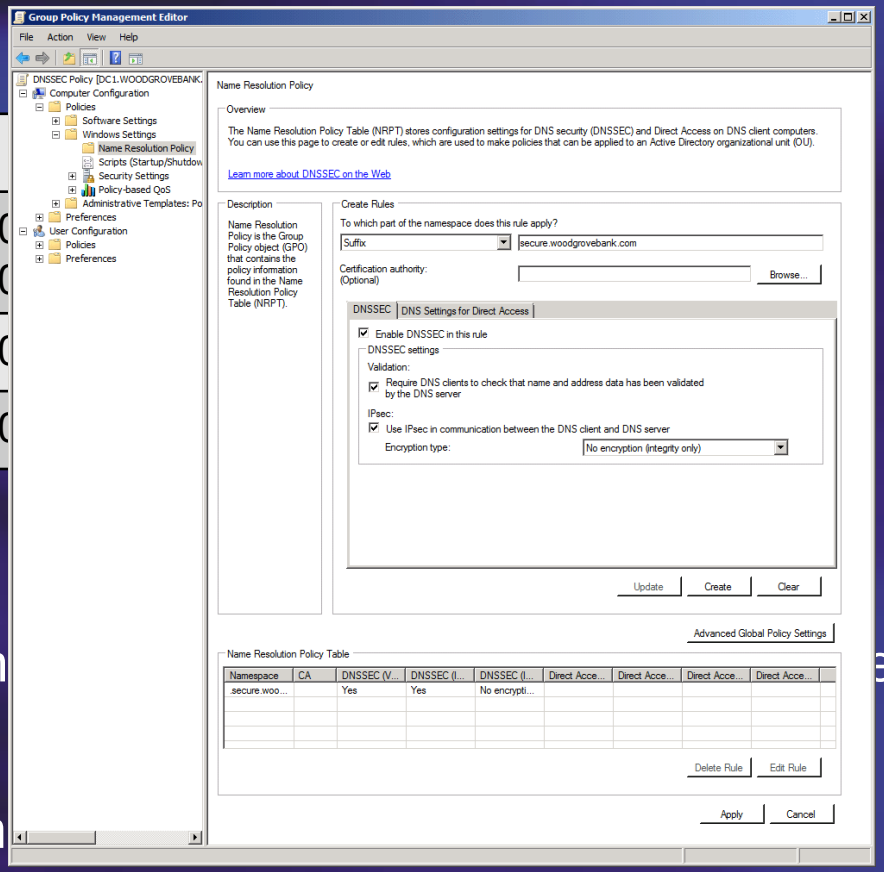


# DNS og Name Resolution Policy Table


- Remote DirectAccess klienter bruger “smart routing” default
- ”Name Resolution Policy Table” tillader at det sker effektivt og sikkert
- Sender navneopslag til interne DNS servere baseret på prekonfigurede DNS namespace

# Name Resolution Policy Table

| NRPT | |
|---|---|
| .ad.contoso.com | 20<br>20 |
| .lab.contoso.com | 20 |
| sql01.acme.com.au | 20 |




- Anvendes på klienten
- Statisk tabel der definerer h… …e ved de listede navne
- Kan ses med kommandoen …
- Konfigureres via GPO - Computer Configuration |Policies|Windows Settings|Name Resolution Policy

# Two Factor Autentification

## *TFA og DirectAccess*

- Intet krav - fuldt supportet
- En bruger kan godt logge på sin pc uden at anvende TFA
- Når brugeren tilgår firma ressourcer
- IPsec authorization policy checker for en kendt SID og hvis det ikke er en kendt SID….

Demo

# DirectAccess

Simpel konfiguration

# Hvordan kommer man i gang?

- DirectAccess: krav
- Infrastructure Planning and Design Guides
- Implementering ”Building end to end trust”

# Krav: DirectAccess

IT Medarbejderes viden
- Basis viden om TCP/IP protokoller, samt IPsec

DirectAccess Klient pc'er
- Windows 7 Enterprise (eller Ultimate)
- "Domain-joined"

DirectAccess Server
- Windows Server 2008 R2
- Står på "kanten" til internettet

# Krav: DirectAccess

Applikations servere
- “End to end” IPv6 eller IPsec kræver Windows Server 2008 eller senere
- Tidligere server versioner kræver NAT-PT

PKI Infrastruktur til at udstede certifikater

DNS Servere, der skal supportere DirectAccess klienter, skal køre Windows Server 2008 SP2 eller senere

Ingen afhængighed af Active Directory version/mode

# Planlægning af DirectAccess

- Start altid her
  - Microsoft Infrastructure Planning and Design
- I tvivl? så søg assistance

# Implementering

***"Building end to end trust"***

- Validering
  - 2 faktor authentikation
  - Active Directory verificeret logon
  - Cached credentials bruges kun offline
- Autorisations politikker
  - Definere tilgang, kryptering og validerings politikker
    - Per server eller per applikation
  - Disse politikker overgår langt traditionelle VPN politikker

# Implementering

***"Building end to end trust"***

- Styring af tilgang til systemerne
  - Auth. firewall (kender bruger identiteter)
  - IPsec
  - Share permissions
  - NTFS permissions
- Overvågning
  - "End to end authentication" tillader at remote klienters forbindelser bliver logget af hver server, der bliver tilgået

# Test

- Brug separate systemer!

# Opsummering

- Giver brugerne transparent adgang til det interne netværks resourcer når de er forbundet til internettet ✓
- Giver IT afdelingen mulighed for at administrere remote computere når de ikke befinder sig på firma netværket ✓
- Etablerer en bi-directional forbindelse der sikrer at klient computeren forbliver opdateret med firma politikker og modtager software opdateringer ✓
- Kræver ikke en VPN forbindelse ✓
- Supporterer multifactor authentication metoder ✓
- Kan konfigureres således at der bestemmes hvilke servere, brugere og individuelle applikationer der er tilgængelige ✓

# Nyttige links

- DirectAccess
  - http://technet.microsoft.com/en-us/network/dd420463.aspx
- DirectAccess Technical Overview
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=64966E88-1377-4D1A-BE86-AB77014495F4&displaylang=en
- Infrastructure Planning and Design Guides
  - http://technet.microsoft.com/en-us/solutionaccelerators/ee382254.aspx

# Spørgsmål

- Q&A

Microsoft®

Your potential. Our passion.™