

# With a little bit of IPv6 magic: Windows 7 DirectAccess

Click to edit Master subtitle style

Thomas Tremel  
Technologieberater  
Microsoft Deutschland GmbH

[Thomas.Tremel@microsoft.com](mailto:Thomas.Tremel@microsoft.com)

# Networking and Access Landscape

## Technology Trends

- Data is walking out the front door and walking in the back door
- Security and access are becoming increasingly complex for IT to manage
- Improving ability to trust end hosts

## Mobile Workforce

- Flexible definition of the “office” – including always remote employees
- Corpnet access from customer sites
- 24x7 work environment demands connectivity from anywhere

## Globalization & Outsourcing

- Others may manage your network and data centers
- Software plus Services augmenting traditional IT – data and applications hosted remotely
- Increasingly complex granular partner access controls
- Users connect from anywhere

## Re-perimeterization of the network is gaining traction

- Traditional Perimeter security is not sufficient alone
- Data center becomes only trusted network
- Shift to protection to host and data level
- Integration of health, access, identity, compliance, and data security solutions
- Emergence of new technology enablers such as IPv6, mobile broadband, and IPsec

# DirectAccess

Providing seamless, secure access to  
enterprise resources from anywhere



# What is Direct Access?

- ▶ Simultaneous corpnet and Internet Access
  - ▶ If user's machine is connected to internet, it is connected to corporate network
- ▶ Remote Management
  - ▶ User's machine is maintainable whenever connected to corporate network over internet
- ▶ Secure remote connectivity
  - ▶ Communication between user's machine and corporate resources is secure

# Internet

DirectAccess Client

DirectAccess Server

Tunnel over IPv4 UDP,  
HTTPS, etc.

Encrypted IPsec+ESP

Encrypted IPsec+ESP

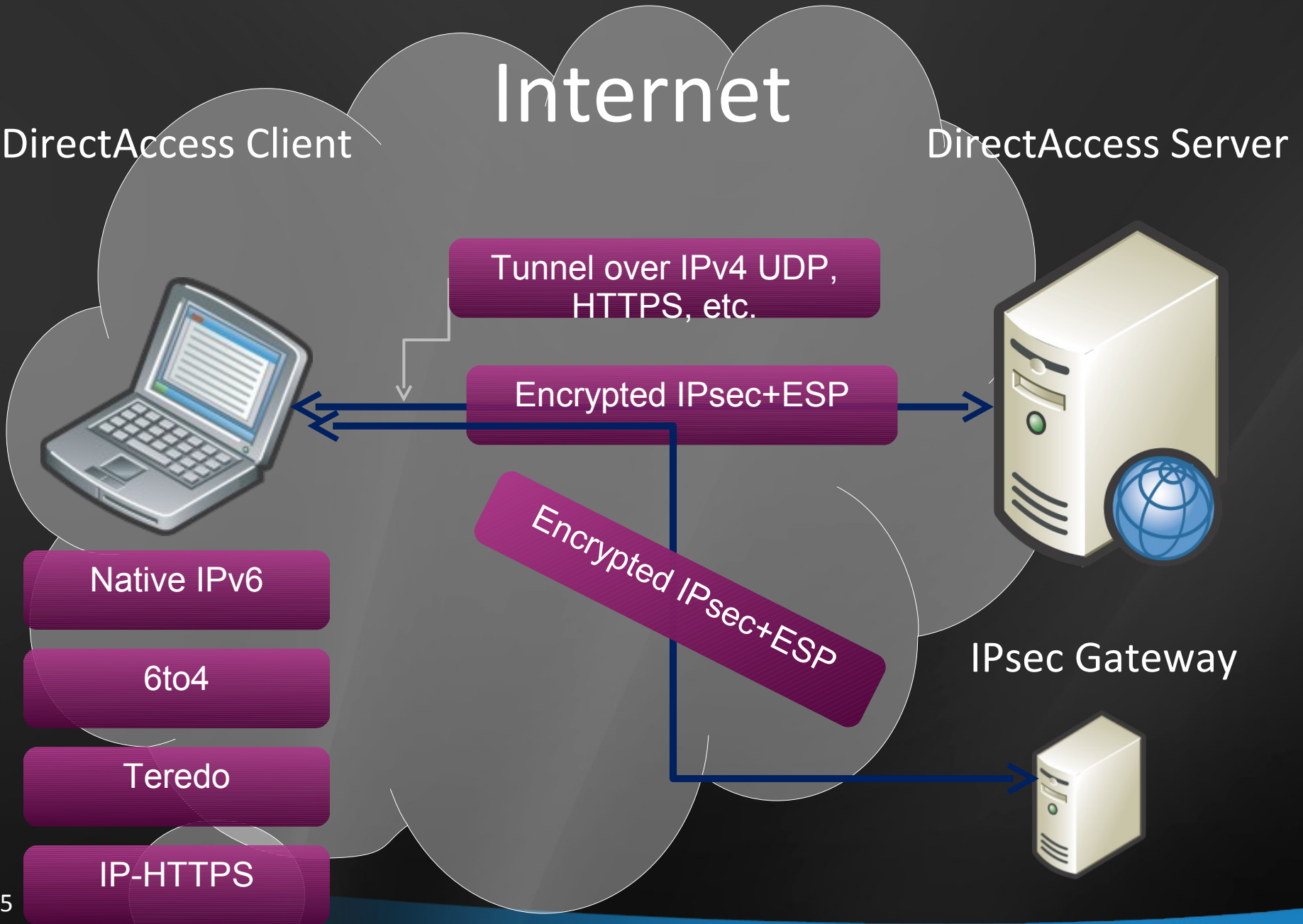
Native IPv6

6to4

Teredo

IP-HTTPS

IPsec Gateway



# Enterprise Network

DirectAccess Server

Line of Business Applications



No IPsec

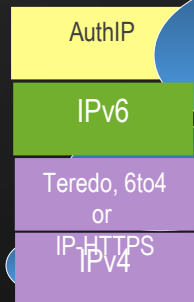
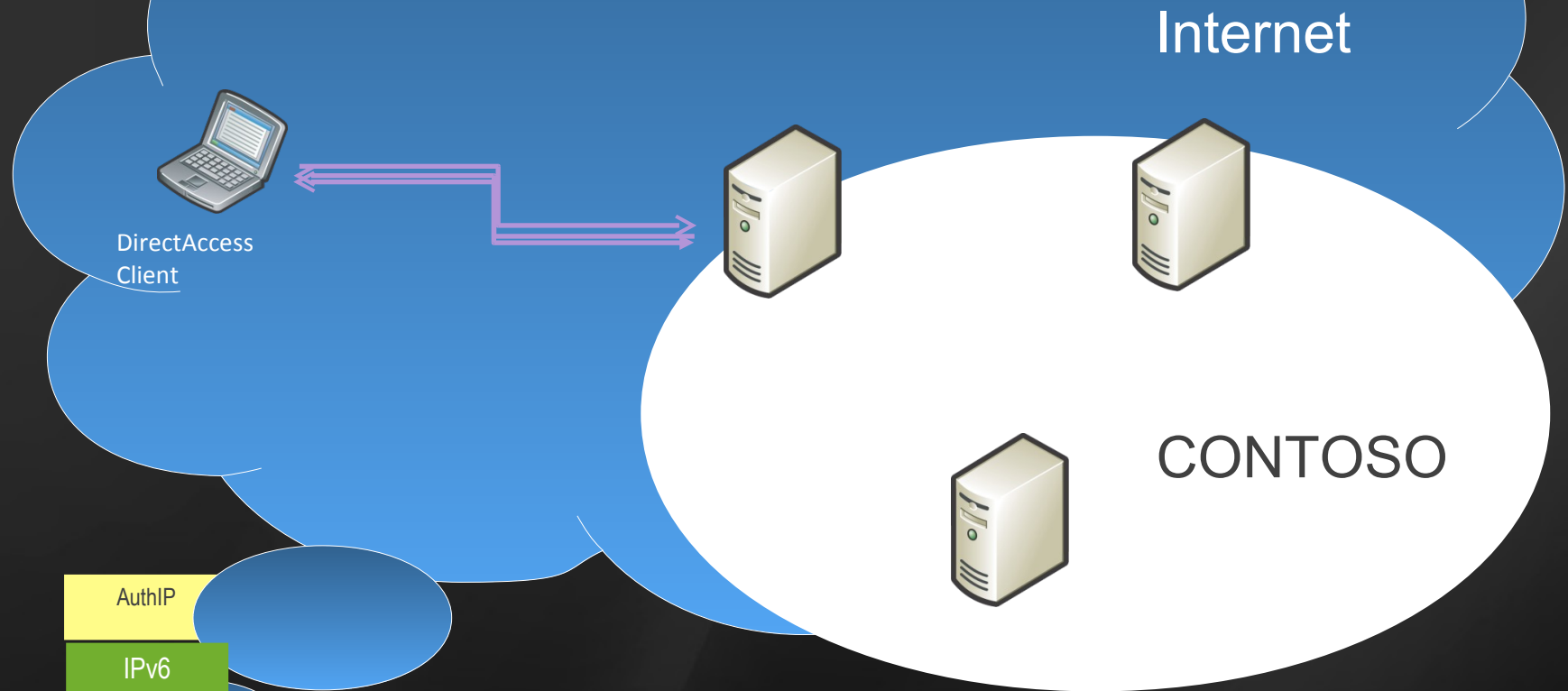
IPsec Integrity  
Only (Auth)

IPsec Integrity +  
Encryption

IPsec Gateway



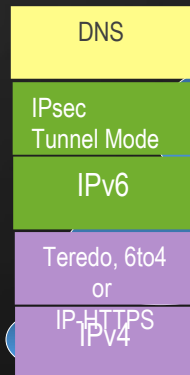
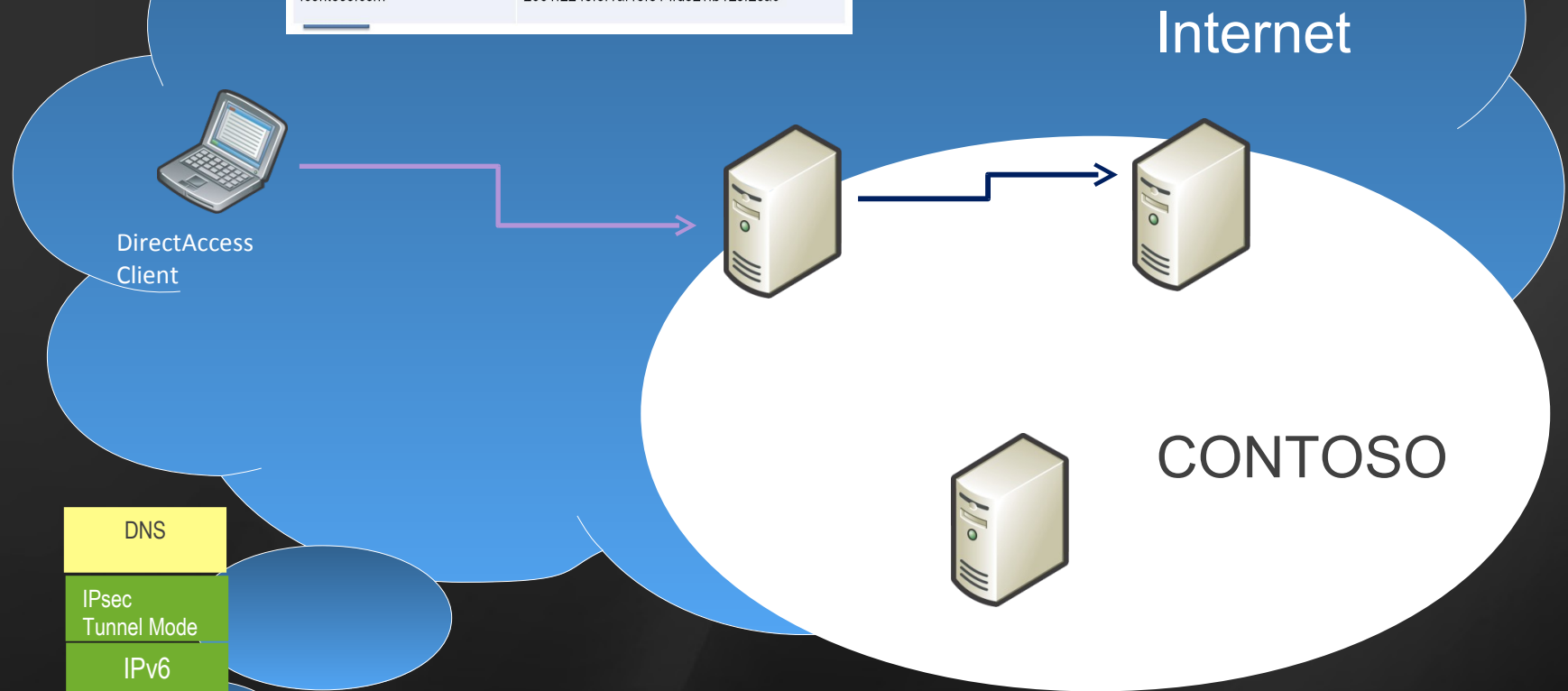
# How DirectAccess Works – Connecting to DA Server



1. Direct Access Client send IPv6 Router Solicitation request to DA Server, using IP-HTTPS, Teredo or 6to4 to communicate over the IPv4 Internet
2. DA Server sends IPv6 Router Advertisement message to DA Client providing it an IPv6 address
3. DA Server authenticates DA Client using AuthIP and establishes IPsec Tunnel between them

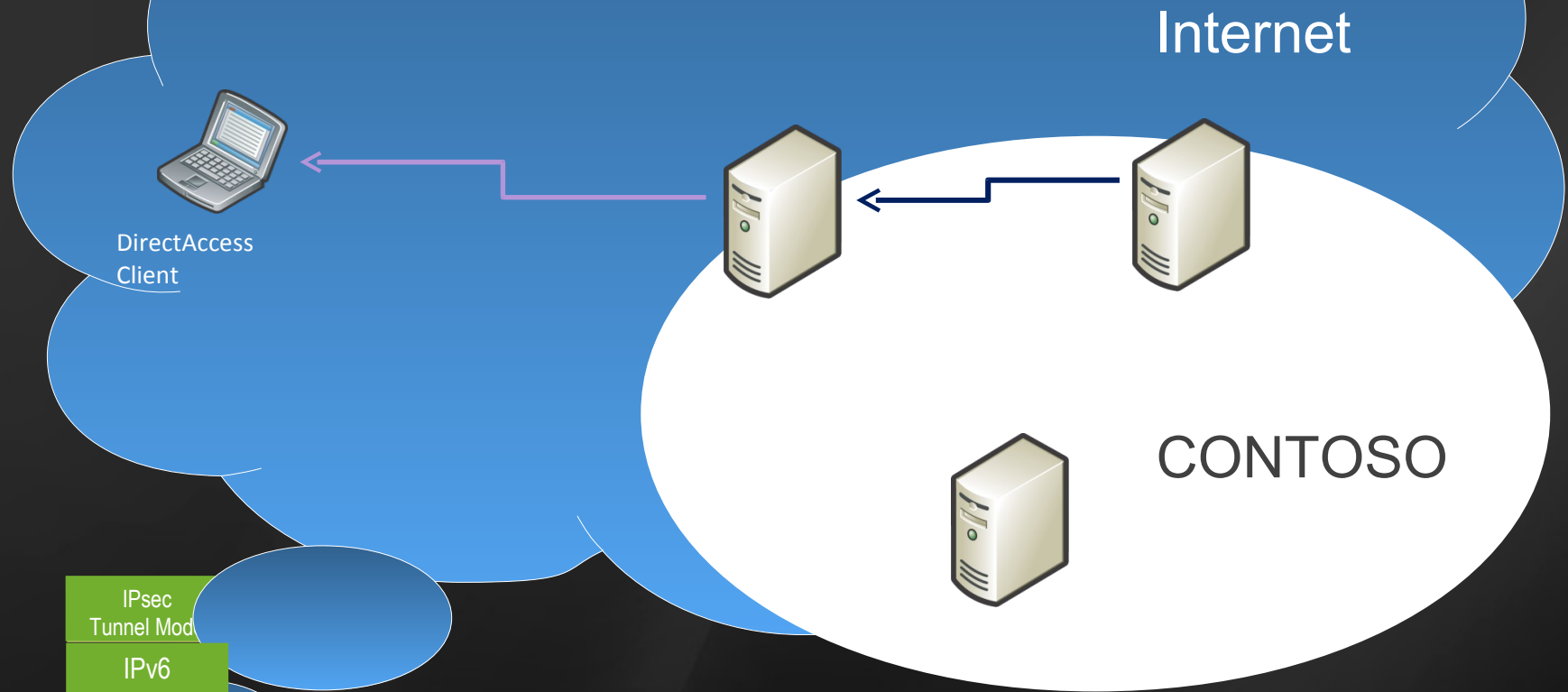
# How DirectAccess Works – Querying DNS

Namespace	DNS Servers
.corp.contoso.com	2001:2245:3f1a:15:314:d321:b020:112a; 2001:2245:3f1a:15:314:d321:b020:114b
.contoso.com	2001:2245:3f1a:15:314:d321:b123:23ac



4. DA Client uses Name Resolution Policy Table (NRPT) to identify which DNS server to query for “server1.corp.contoso.com”
5. DA Client send query to DNS Server through the IPsec tunnel established with the DirectAccess Server
6. DA Server terminates IPsec tunnel and forwards packet to internal DNS Server

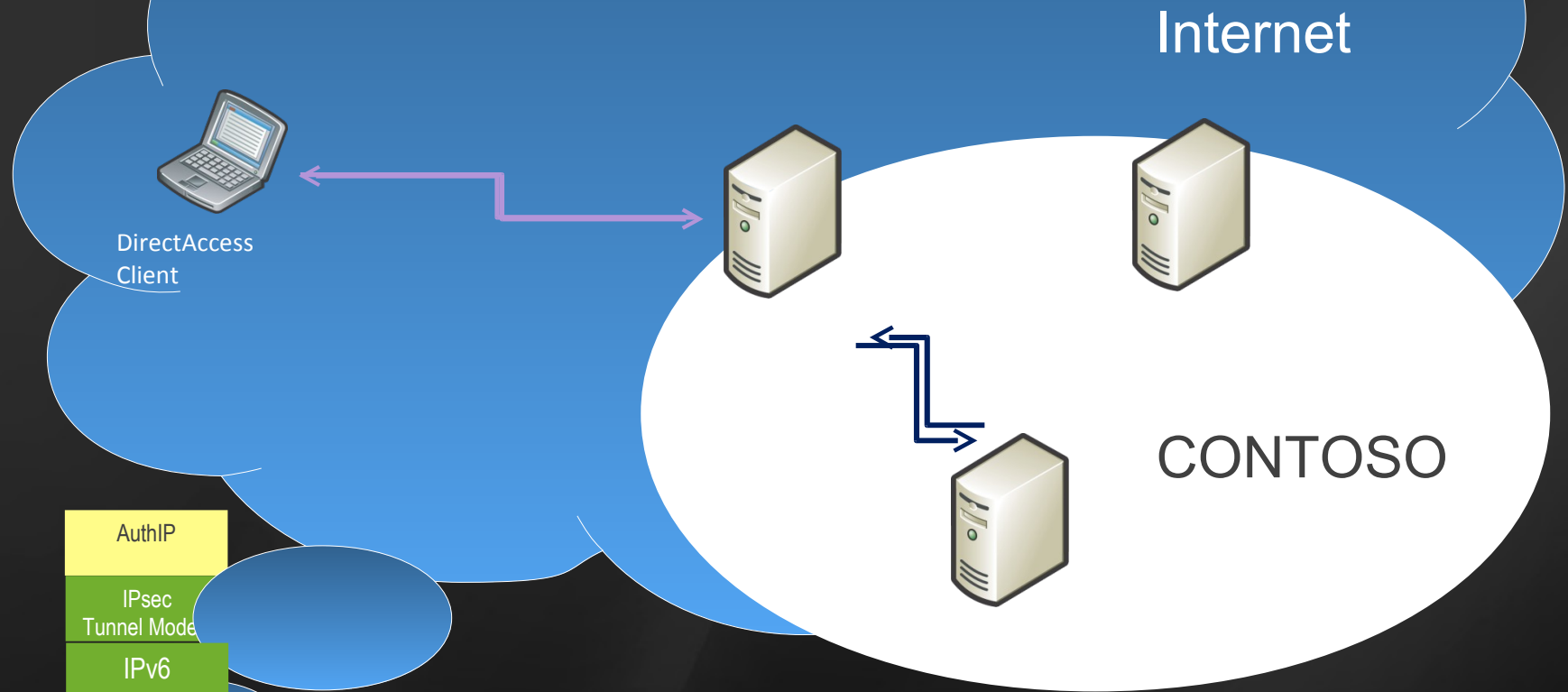
# How DirectAccess Works – Querying DNS



- IPsec Tunnel Mod
- IPv6
- Teredo, 6to4 or IP-HTTPS
- IPv4

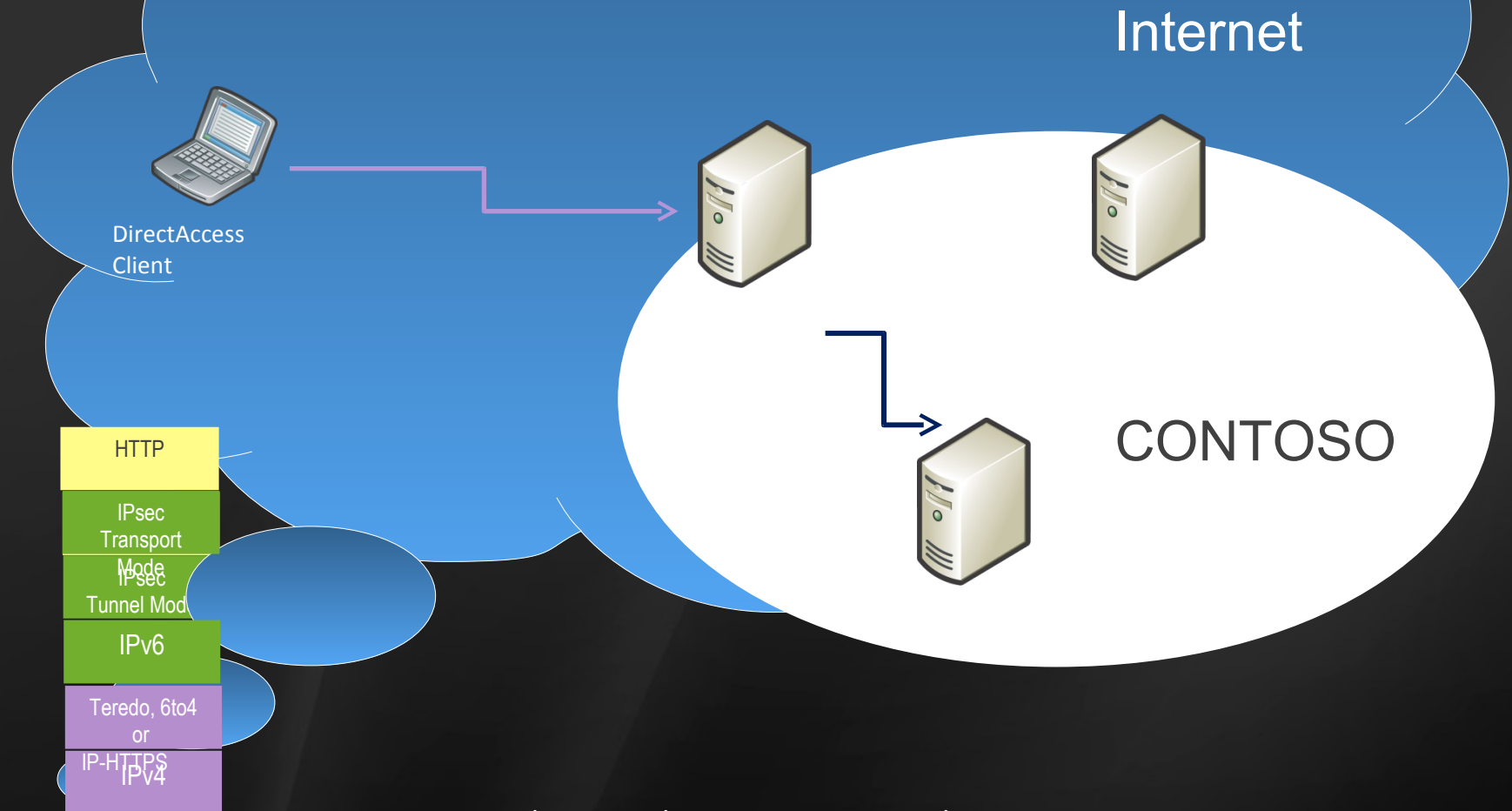
7. DNS Server replies back with IPv6 address for “server1.corp.contoso.com”
8. DA Server sends DNS reply to DA Client over IPsec tunnel

# How DirectAccess Works – Connecting to Internal Server



9. DirectAccess Client authenticates to Server1 server using AuthIP and establishes IPsec Transport Mode security association

# How DirectAccess Works – Connecting to Internal Server

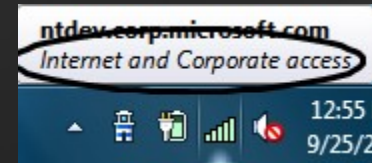


10. DirectAccess Client user browses content on the Server1 server



# Inside/Outside Determination

- ▶ DA client needs to determine whether they are inside or outside the corporate network
  - ▶ Impacts Windows Firewall and IPsec policies, Network Connections UI



Status determined by probing internal Web site

- ▶ Only needs to provide a connection; it does not need to be hosting any special software or configured in any particular way
- ▶ URL configured on the client registry

# Name Resolution Policy Table

## (NRPT)

- Allows DirectAccess clients to use internal DNS servers
  - Clients can query explicitly defined DNS servers for different DNS namespaces
  - Optionally, DNS queries for specific namespaces can be secured using IPsec

Namespace	DNS Servers
.int.company.com	2001:2245:3f1a:15:314:d321:b020:112a; 2001:2245:3f1a:15:314:d321:b020:114b
.corp.company.com	2001:2245:3f1a:15:314:d321:b123:23ac

- New Windows 7 feature

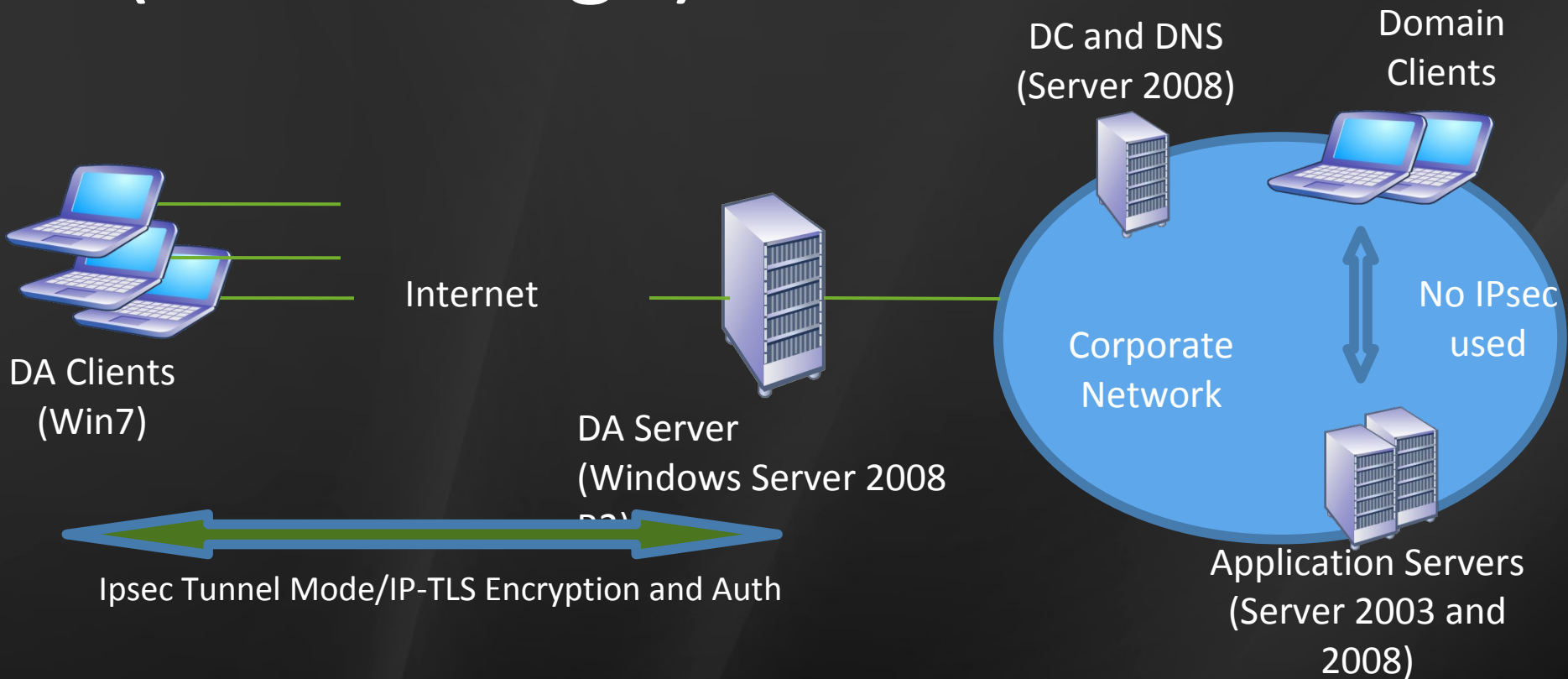
# IPsec Gateway

- ▶ IPsec connectivity endpoint for DA clients
  - ▶ Terminates IPsec Tunnel Mode connection
  - ▶ Authenticates DA client before it can reach the internal resources (optionally requiring smart card certificate)
  - ▶ Hosted on DA server by default, can be moved to different server
- ▶ IPsec Gateway also provides IPsec DoS Prevention
  - ▶ Prevents DoS attacks that can be inflicted via exploitations from key management protocols (IKE, AuthIP, etc.)
  - ▶ Defines maximum rate for received requests

# Direct Access Deployment Scenarios

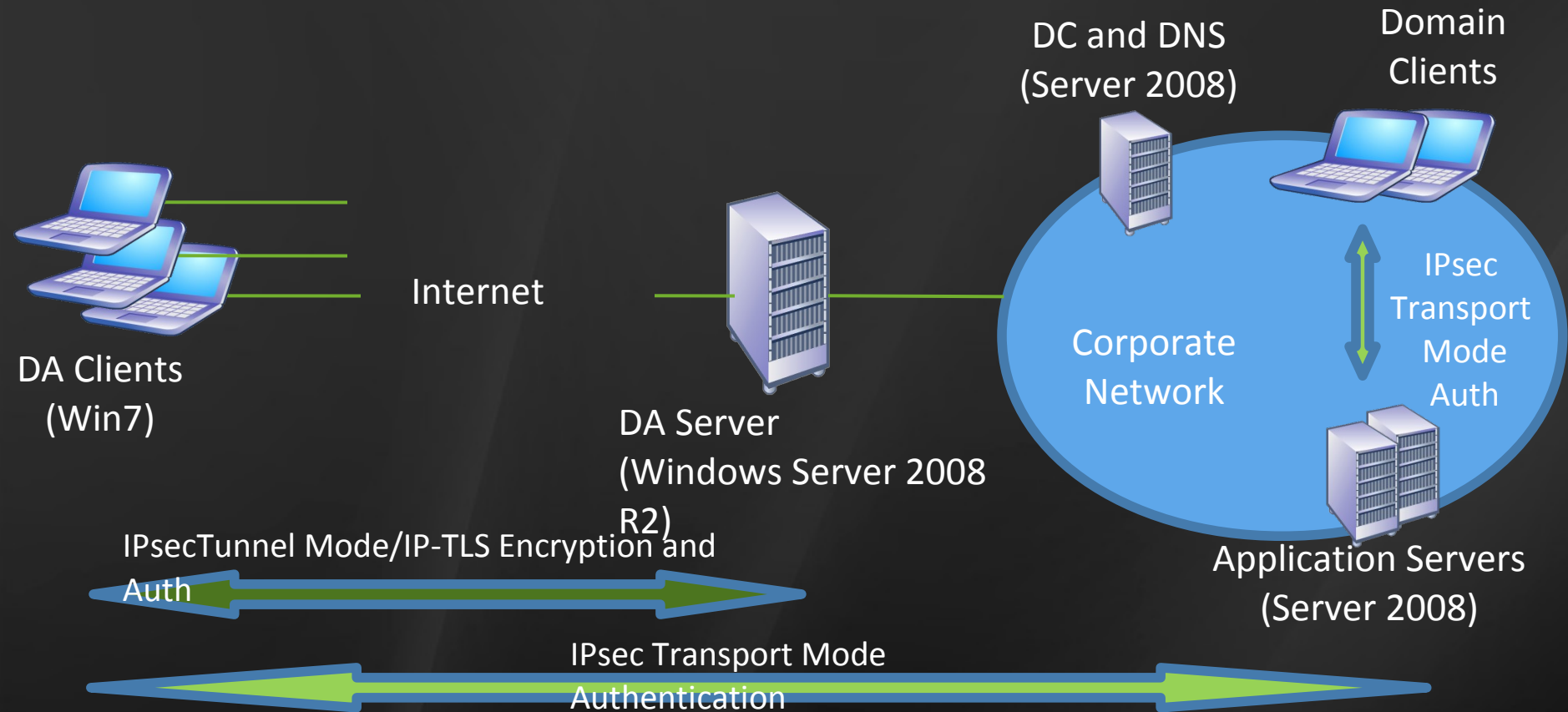
- ▶ Full Intranet Access Model
- ▶ Selected Server Access Model
- ▶ End to End Access Model

# Full Intranet Access Model (End to Edge)



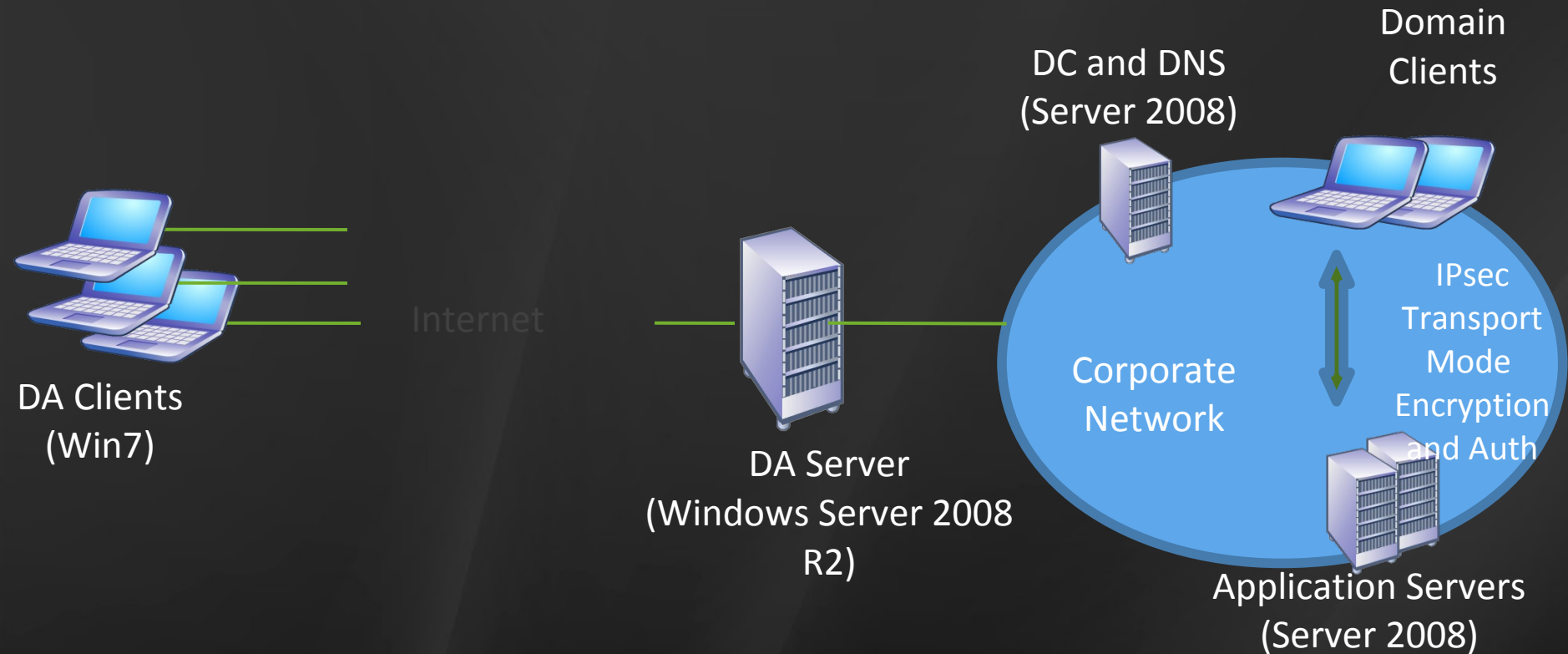
- Architecture similar to current VPN deployments
- Works with any IPv6 capable servers, including Windows Server 2003

# Selected Server Access Model (End to Edge modified)



- Fine grained control over which resources are available
- Servers must be running Windows Server 2008 or later

# End to End Access Model



IPsec Transport Mode Encryption and Authentication

- IPsec policies established end-to-end to the application servers
- DA Server/IPsec Gateway acting simply as a passthrough

# DirectAccess Deployment Requirements

- ▶ Microsoft Windows 7 clients
- ▶ Microsoft Windows 2008 R2 DA server
- ▶ Application servers
  - ▶ End-to-end encryption requires Windows Server 2008 or later; other models can use Windows Server 2003 or later
  - ▶ Must have an IPv6 address
- ▶ DC/DNS servers
  - ▶ Windows Server 2008 (with hotfix)
  - ▶ Two-factor authentication for end-to-end auth requires AD in Windows Server 2008 R2 domain functional level
- ▶ NAT-PT server if IPv4 access is desired

# Infrastructure Requirements

- ▶ Active Directory domain required
  - ▶ One DC should be running Windows Server 2008 or later
  - ▶ A security group needs to be created for the DA clients
- ▶ Public Key Infrastructure (PKI) required
  - ▶ External trust is not required
  - ▶ SSL certificates must have a CRL distribution point that is reachable via a publicly resolvable FQDN
- ▶ IPv6 connectivity required
  - ▶ DirectAccess clients can only communicate with internal servers and resources that have IPv6 connectivity
    - ▶ Native connectivity is not required – IPv6 transition technologies may be used

# Why Windows 7 only?

- ▶ Significant component changes for DirectAccess:
  - ▶ Name Resolution Policy Table
  - ▶ IP-HTTPS
  - ▶ Group Policy changes
  - ▶ And others...

# DirectAccess Benefits

## Always-on

Internet connectivity = Enterprise connectivity

Connects automatically

Adapts to changing networks

## Secure

Encrypted by default

Policy-based Application or Server level controls

Fully supports smartcard authentication

## Manageable

Wizard-based installation & policy creation

Allows management of remote clients

## Lower TCO

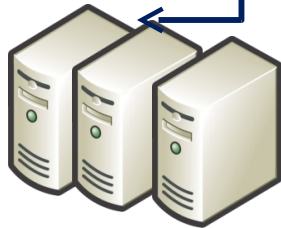
Simplified edge policies

Reduced user overhead

No need for per-application gateways

# Vision

Enterprise  
Network



Assume the underlying network is always insecure

Redefine CORPNET edge to cocoon the datacenter and business critical resources

Users are remote at all times

▶ Questions / Answers

*Your potential, our passion* ™

**Microsoft**®

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.