

# DirectAccess

**Presented by**  
**Joe Davies**  
**Principal Technical Writer**  
**Windows Server User Assistance**

Presented at:  
**Seattle Windows Networking User Group**  
November 5, 2009

# Agenda

- What is it?
- How does it work?
- How do I set it up?

# DirectAccess-What is it?

- Always on, bi-directional seamless connectivity to your intranet
  - Next generation remote access VPN technology
  - Reduces dependence on VPN connections
  - Much easier to "manage-out"
- Key requirements
  - Windows 7 and Windows Server 2008 R2
  - Domain-joined computers

# DirectAccess User Experience

- On the intranet
  - Open laptop computer
  - Access intranet resources via LAN
  - Access Internet resources via intranet Web proxy
- On the Internet
  - Open laptop computer
    - Protected tunnels to the DirectAccess server are automatically created
  - Access intranet resources via DirectAccess connection
  - Access Internet resources via ISP
- Result
  - Same user experience for both environments

# DirectAccess IT Administrator Experience

- On the intranet
  - Open laptop computer
  - Updates Group Policy, installs updates
  - Accessible for remote administration
- On the Internet
  - Open laptop computer
  - Updates Group Policy, installs updates
  - Accessible for remote administration
- Result
  - Same IT administrator experience for both environments
  - Mobile nodes remain in compliance

# DirectAccess-How does it work?

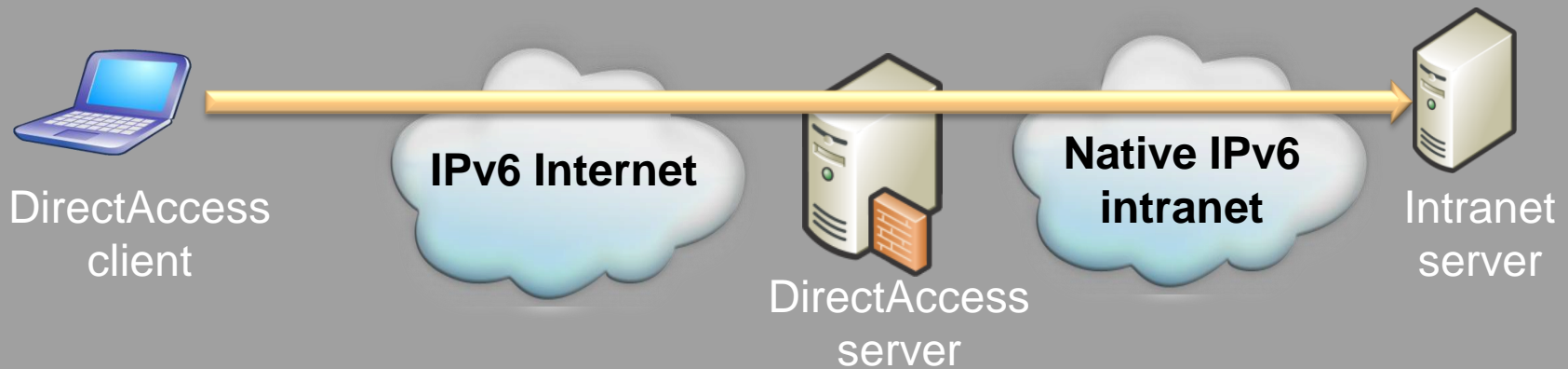
- Arthur C. Clarke's Third Law
  - *"Any sufficiently advanced technology is indistinguishable from magic."*
- DirectAccess magic-enabling technologies
  - Internet Protocol version 6 (IPv6)
  - Internet Protocol security (IPsec)
  - The Name Resolution Policy Table (NRPT)
  - Network location detection

# Magic-enabler: IPv6

- Internet Engineering Task Force (IETF) standard replacement for IPv4 in TCP/IP
  - Extended addressing, but so much more
- New features of IPv6 for Windows 7
  - IPv6 transition technology configuration via Group Policy
- Why IPv6?
  - DirectAccess is a forward-looking technology
  - IPv6 provides global addressing and end-to-end connectivity for DirectAccess
    - Inherent problems with IPv4 and overlapping address spaces

# Ideal DirectAccess Environment

- IPv6 Internet and native IPv6 intranet



# Real World DirectAccess Environment

- IPv4 Internet and IPv4-only intranet



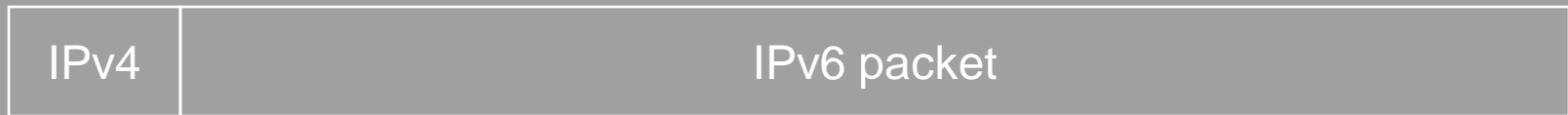
# Getting IPv6 Traffic Across IPv4-only Networks

TechNet Events

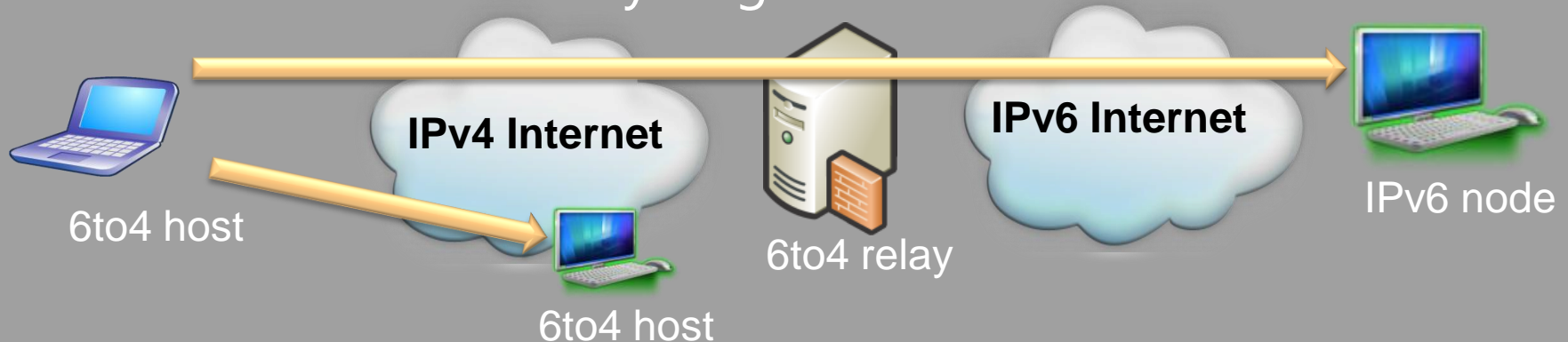
- IPv6 transition technologies
  - Encapsulating IPv6 packets as IPv4 packets
- Across the IPv4 Internet
  - 6to4
  - Teredo
  - IP-HTTPS
- Across an IPv4-only intranet
  - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

# 6to4

- IPv4 protocol 41 encapsulation



- 6to4 host
  - Requires a public IPv4 address
  - Uses a 6to4 relay to get to the IPv6 Internet



# Teredo

- IPv4+UDP encapsulation



- Teredo client
  - Can be behind a NAT with a private IPv4 address
  - Uses a Teredo server and relay to self-configure and get to the IPv6 Internet

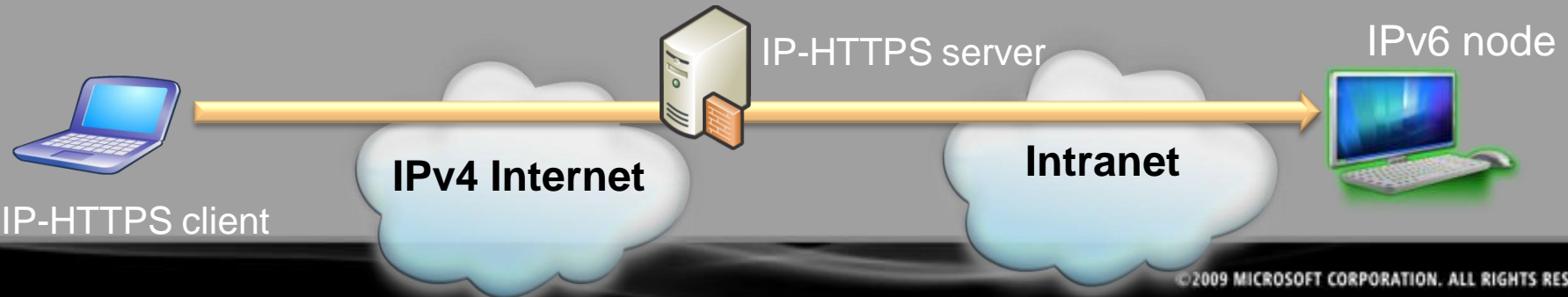


# IP-HTTPS

- New protocol for Windows 7/Windows Server 2008 R2
- IPv4+HTTPS encapsulation

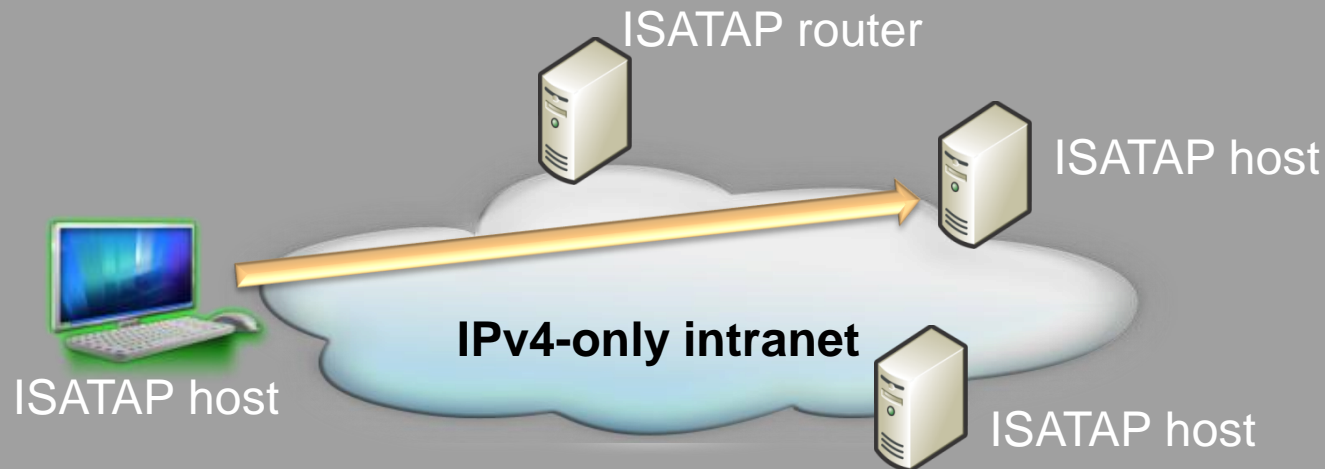


- DirectAccess client
  - Uses IP-HTTPS when 6to4 and Teredo connectivity are not available
  - Uses an IP-HTTPS server to access an intranet



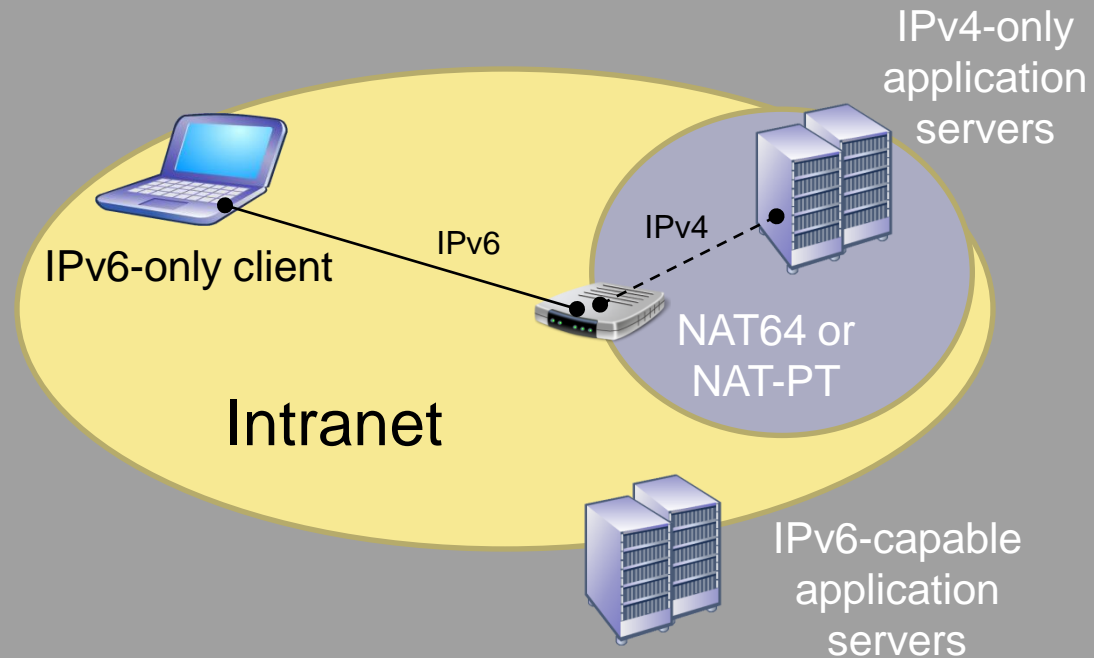
# ISATAP

- IPv4 protocol 41 encapsulation
- Used on the IPv4-only portion of an intranet
  - Treats an IPv4-only infrastructure as a single subnet
- Windows-based ISATAP hosts locate the ISATAP router by resolving the name "isatap"



# Getting IPv6 Traffic to IPv4-only Endpoints

- Translating IPv6 and IPv4 traffic
  - NAT64
  - Network Address Translation-Protocol Translation (NAT-PT)



# Summary of IPv6 for DirectAccess

- DirectAccess requires IPv6 end-to-end
  - DirectAccess client only sends IPv6 traffic
  - Intranet resource must be
    - IPv6-capable (native IPv6 or ISATAP)
    - Reachable via NAT64 or NAT-PT
- DirectAccess clients use 6to4, Teredo, or IP-HTTPS to send IPv6 packets to the DirectAccess server across the IPv4 Internet
- You can use ISATAP on your intranet while you deploy native IPv6

# Magic-enabler: IPsec

- IETF standard for protecting IP traffic (IPv4 and IPv6)
  - Peer authentication, data integrity, and data confidentiality (encryption) at the Internet layer
- IPsec modes
  - Transport mode: protect the packet payload
  - Tunnel mode: protect the entire packet
- DirectAccess and IPsec
  - Tunnel mode to encrypt traffic across the Internet
  - Transport mode to protect traffic to intranet resources

- Connection security rules in Windows Firewall with Advanced Security
  - Rule example:
    - For traffic to HRSRV1, authenticate using Kerberos computer credentials, use SHA-1 for data integrity, and AES-128 for data confidentiality
- New features of IPsec for Windows 7 and Windows Server 2008 R2 for DirectAccess
  - Dynamic tunnel endpoints
  - Tunnel authorization
  - Authentication with null encapsulation

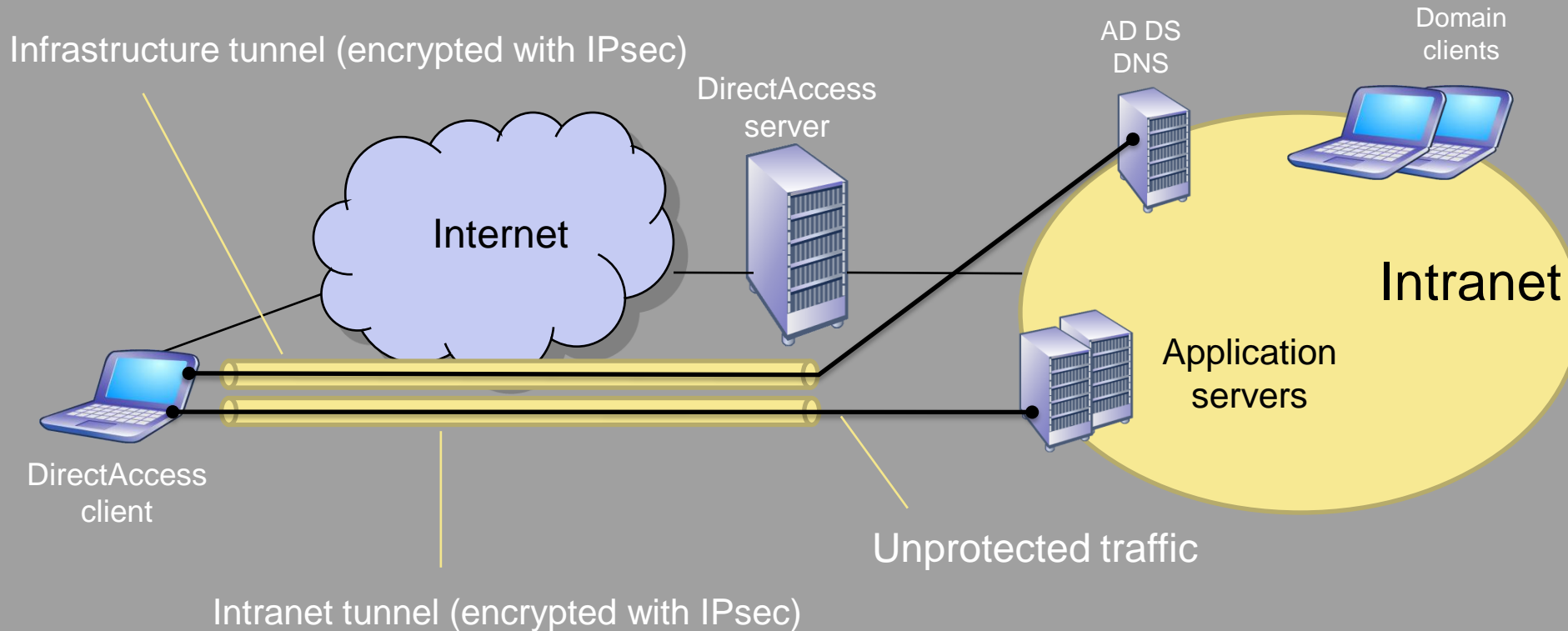
# DirectAccess Deployment Models

TechNet Events

- Full intranet access
- Selected server access
- End-to-end access

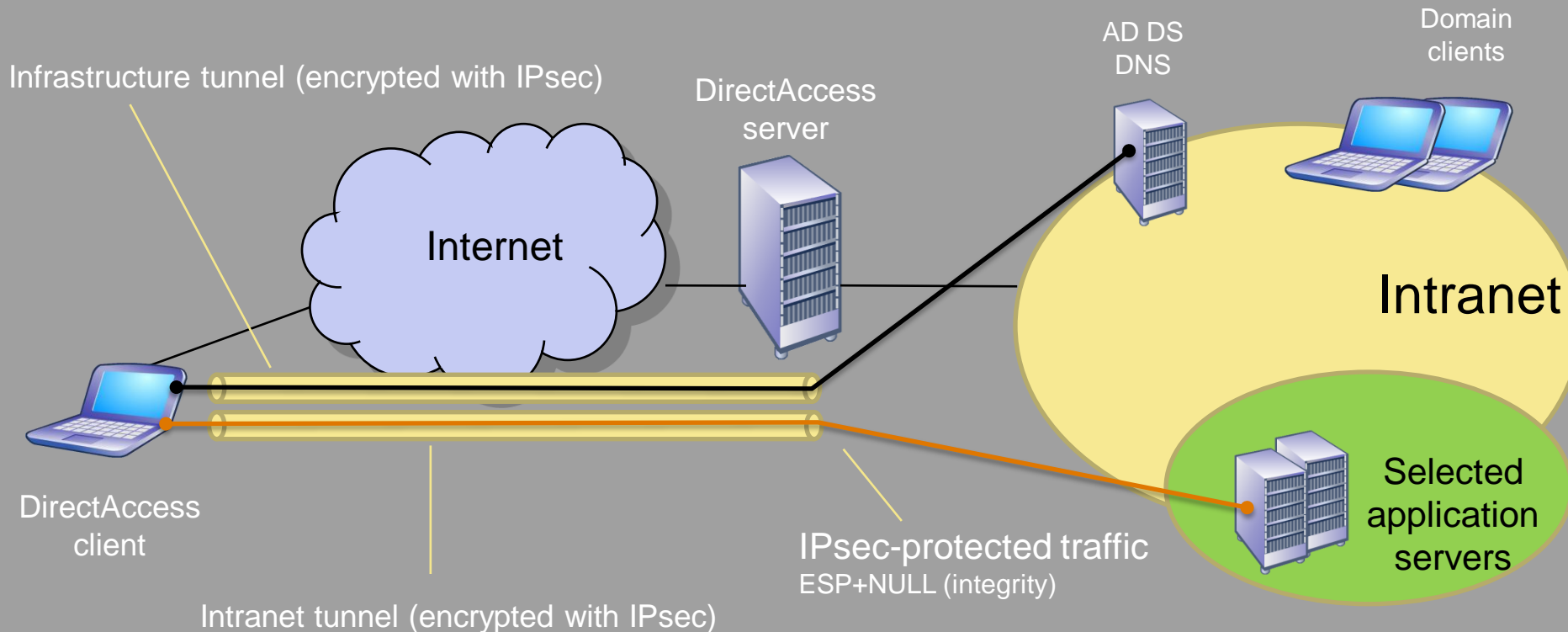
# Full Intranet Access Model

- IPsec tunnel mode encryption over the Internet
- No protection of traffic on the intranet



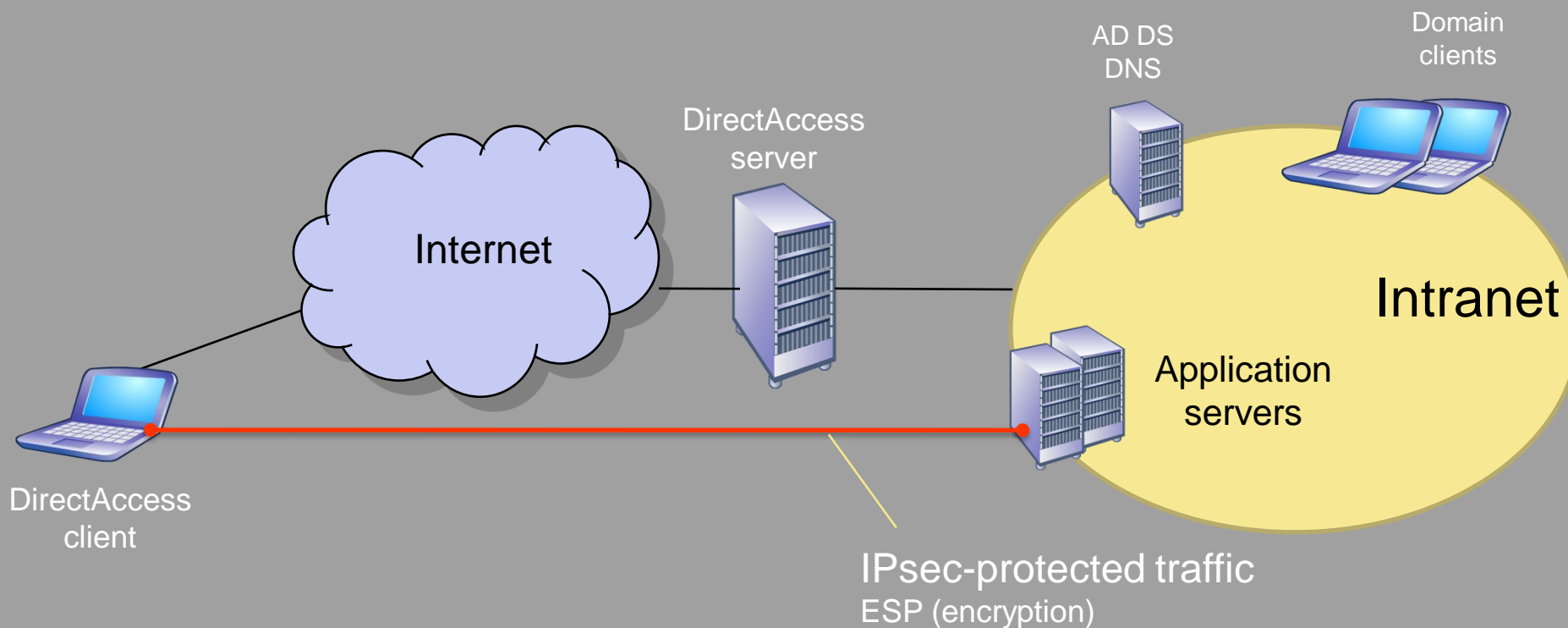
# Selected Server Access Model

- IPsec tunnel mode encryption over the Internet
- IPsec transport mode data integrity for traffic to specified servers on the intranet (exclusive or non-exclusive)



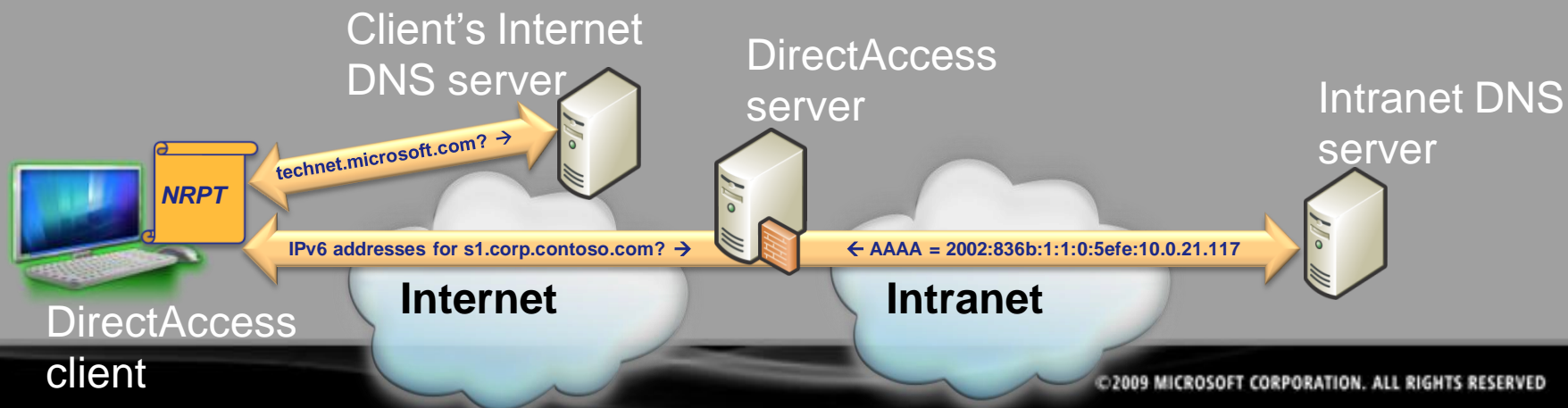
# End-to-end Access Model

- IPsec transport mode encryption for all intranet traffic



# Magic-enabler: NRPT

- New to Windows 7 and Windows Server 2008 R2
- DNS Client service table for special handling of DNS queries
  - DirectAccess
  - DNS Security Extensions (DNSSEC)
- For DirectAccess, acts as a client-side conditional forwarder
  - Determines which names should be directed to which DNS servers



# NRPT and DirectAccess

- For intranet FQDNs, send IPv6-specific name queries to the IPv6 address of an intranet DNS server
  - Returns only AAAA records
- For other FQDNs, send general name queries to interface-configured DNS servers
- Exemption rules for specific FQDNs that match the intranet namespace

<b>NRPT</b>	
.corp.contoso.com	2002:836b:1:1:0:5efe:10.1.1.99 2002:836b:1:1:0:5efe:10.1.1.100

# Magic-enabler: Network Location Detection

- Firewall profile determination
  - The attached networks and their profiles
- Intranet detection
  - Whether the DirectAccess client is directly connected to the intranet

# Firewall Profile Determination

- Network Location Awareness service determines
  - The attached networks
  - Their profile type (public, private, domain)
- New to Windows 7 and Windows Server 2008 R2
  - Multiple active firewall profiles
- DirectAccess connection security rules for IPsec protection are specified for the public and private profiles only

# Intranet Detection

- Also known as inside/outside detection
- Tests access to an intranet-only HTTPS-based URL
- When on the intranet
  - Don't use DirectAccess rules in the NRPT (normal intranet access)
- When **not** on the intranet
  - Use DirectAccess rules in the NRPT to separate DNS queries

# Putting the Magic All Together

- Let's examine the role of IPv6, IPsec, the NRPT, and network location detection for a DirectAccess client
  - On the intranet
    - Expected result is normal intranet access
  - On the Internet
    - Expected result is tunneled, encrypted, and separated intranet access

# DirectAccess Client on the Intranet

- DirectAccess client assumes that it is not on the intranet
  - Connection security rules are active and DirectAccess NRPT rules are present
- Network Location Awareness service determines that an attached network is in the domain profile
  - Connection security rules are deactivated
- DirectAccess client accesses intranet HTTPS-based URL
  - DirectAccess rules are removed from the NRPT
- DirectAccess client has normal intranet access

# DirectAccess Client on the Internet

- DirectAccess client assumes that it is not on the intranet
  - Connection security rules are active and DirectAccess NRPT rules are present
- Network Location Awareness service determines that the attached networks are only in the public and private profiles
  - Connection security rules remain active
- DirectAccess client cannot access intranet HTTPS-based URL
  - DirectAccess rules remain in the NRPT
- DirectAccess client uses the NRPT and connection security rules to create tunnels, resolve intranet FQDNs, and access intranet resources

# DirectAccess-How Do I Set it Up?

- Infrastructure components
- DirectAccess server and client requirements
- Before running the DirectAccess Setup Wizard
- The DirectAccess Setup Wizard
- DirectAccess deployment options

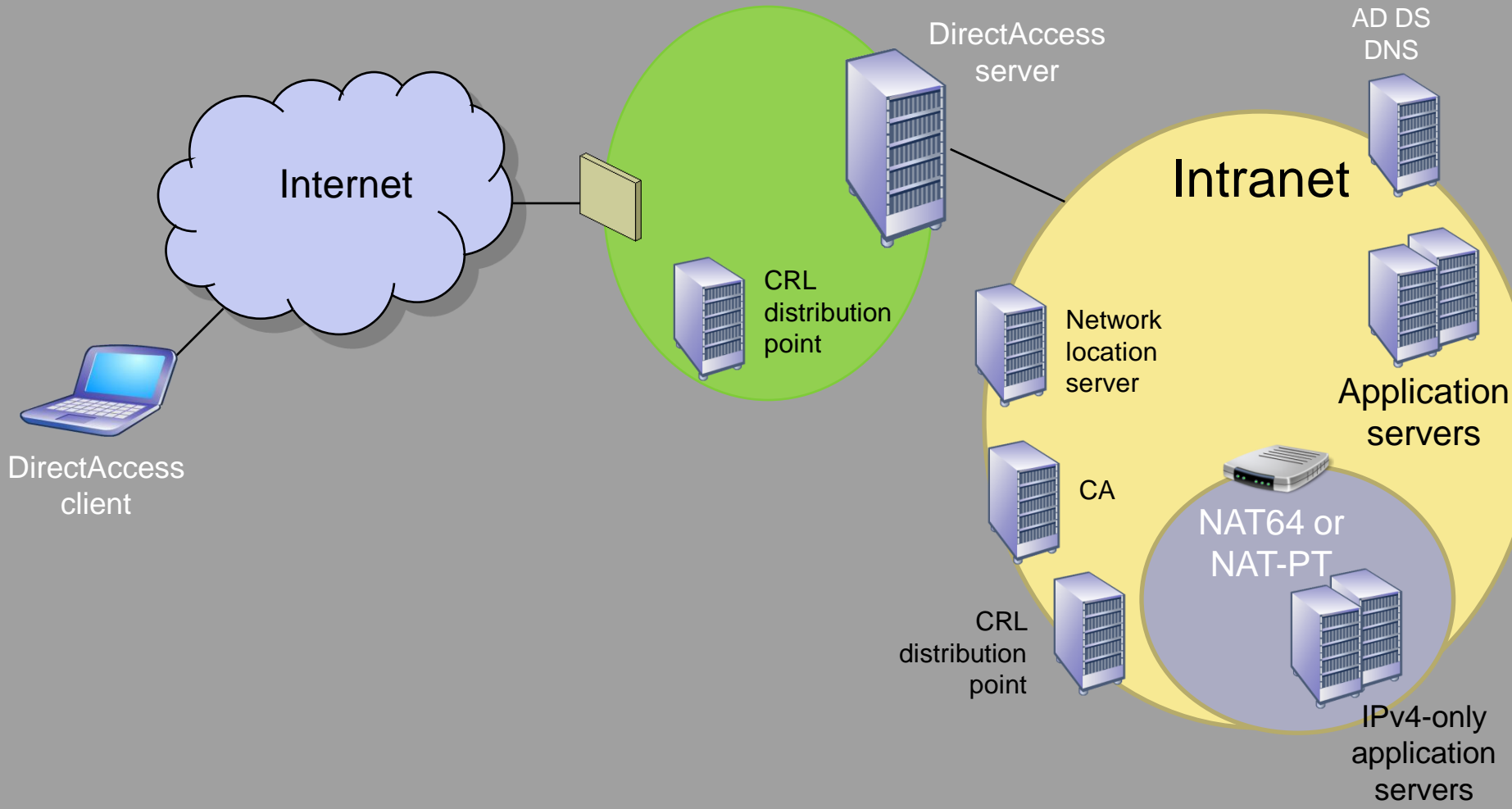
# DirectAccess Infrastructure Components

- Active Directory Domain Services
  - At least one IPv6-capable DC for DirectAccess clients (Windows Server 2008 or later)
- DNS
  - At least one ISATAP and IPv6-capable DNS server for DirectAccess clients (Windows Server 2008 Service Pack 2 or later)
- Certification Authority (CA)
  - Certificates for DirectAccess clients, DirectAccess servers, network location server
  - CRL distribution points for the intranet and Internet

# DirectAccess Infrastructure Components (cont.)

- Network location server
  - Web server capable of hosting an HTTPS URL
- DirectAccess server
- DirectAccess clients
- NAT64 or NAT-PT (optional)

# DirectAccess Deployment



# DirectAccess Server Requirements

- Windows Server 2008 R2 or later
- Member of an AD DS domain
- At least two network adapters that are connected to the Internet and your intranet
- 2 consecutive, public IPv4 addresses configured on the Internet network adapter
- Certificates
  - Computer certificate for IPsec authentication
  - Secure Sockets Layer (SSL) certificate for IP-HTTPS

# DirectAccess Client Requirements

- Windows 7 Ultimate Edition, Windows 7 Enterprise Edition, Windows Server 2008 R2
- Member of an AD DS domain
- Computer certificate for IPsec authentication

# Before Running the DirectAccess Setup Wizard

- AD DS
  - Security groups for DirectAccess clients (required) and selected servers (optional)
- Internet firewall
  - Packet filters to allow 6to4, Teredo, and IP-HTTPS traffic
- PKI
  - Autoenrollment for computer or other certificates
  - Internal and external CRL distribution points
  - Additional SSL certificate on the DirectAccess server
- Web
  - Create HTTPS-based network location URL
- DNS
  - Remove ISATAP from global query block list

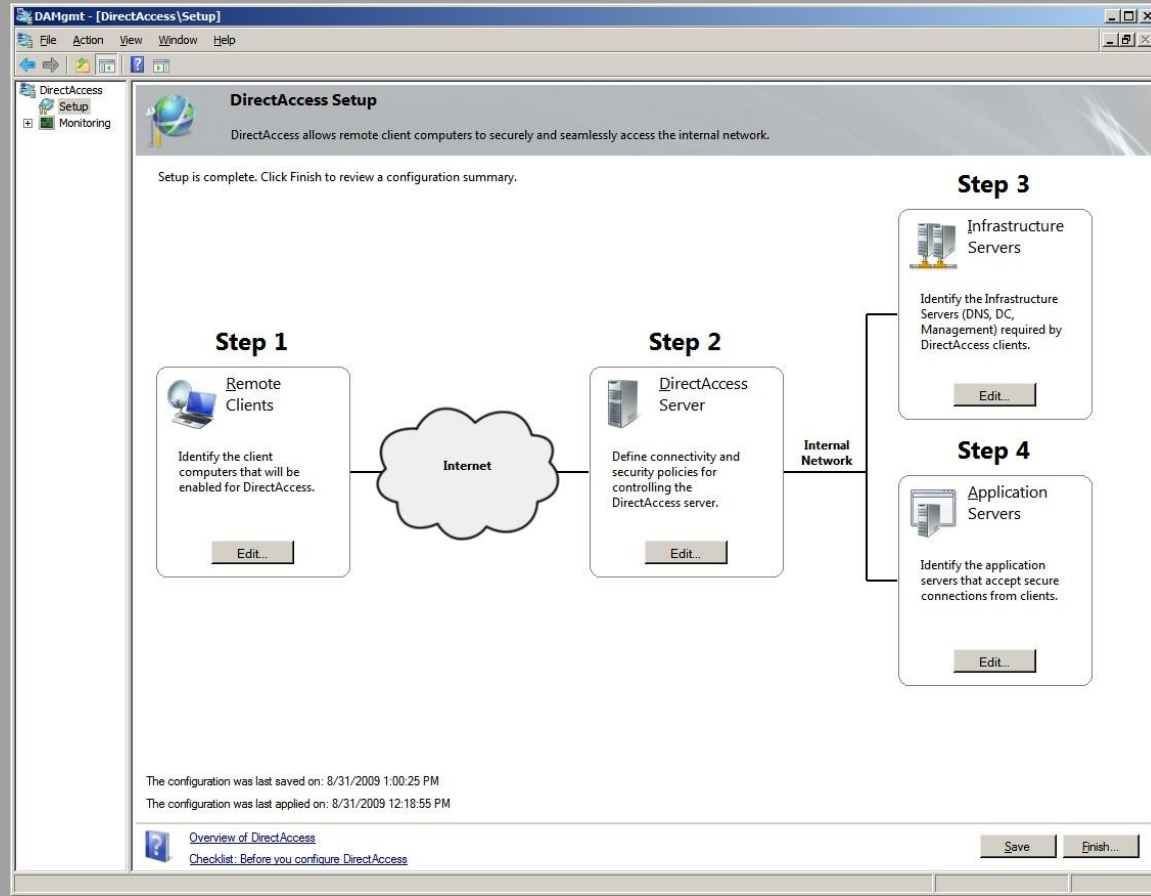
# Installing and Configuring DirectAccess

- Install the DirectAccess Management Console feature with Server Manager
- DirectAccess Management administrative tool
  - Setup node
    - Run the DirectAccess Setup Wizard
  - Monitoring node
    - Monitor components of DirectAccess on the server

# Demo

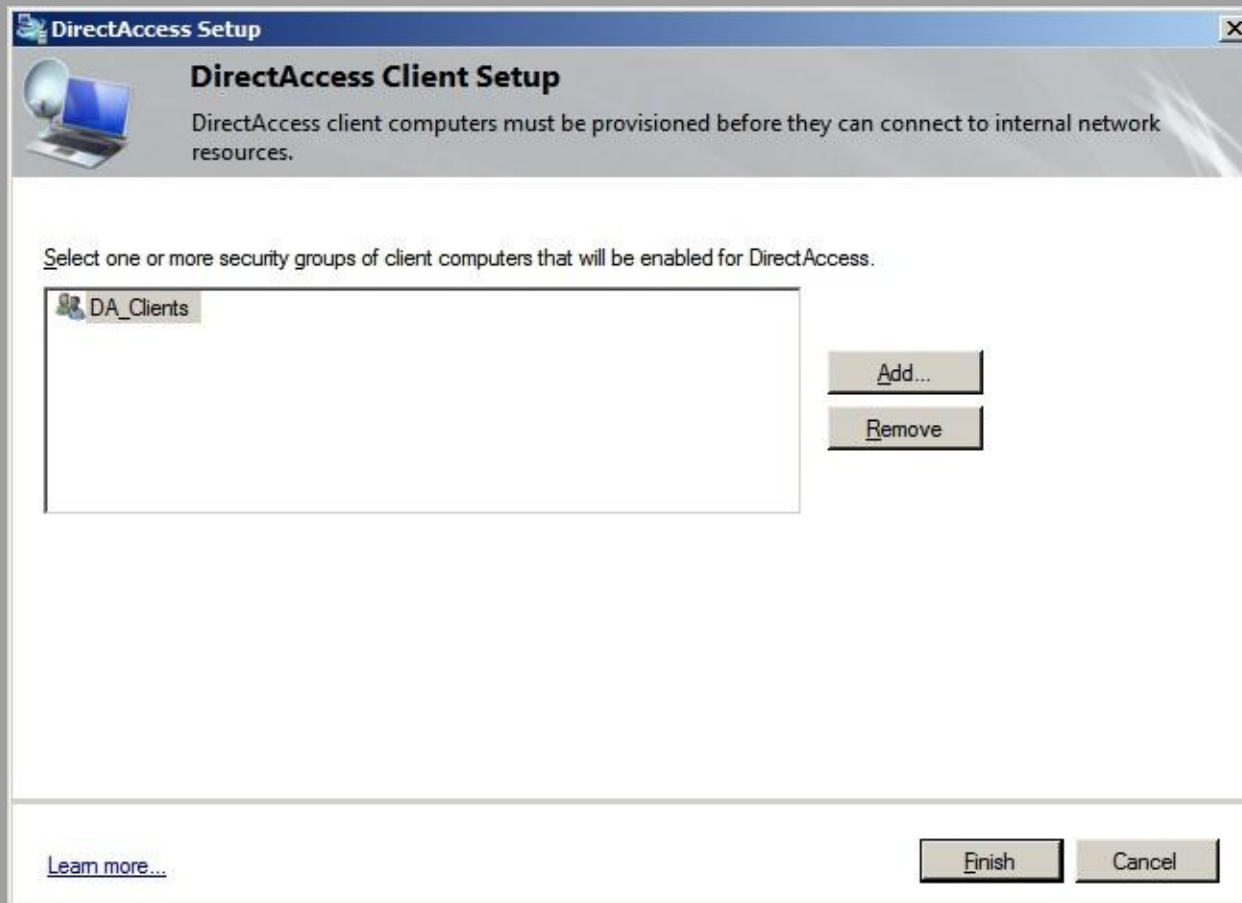
# DirectAccess Setup Wizard

- Step 1
  - DirectAccess clients
- Step 2
  - DirectAccess server
- Step 3
  - Infrastructure servers
- Step 4
  - Application servers



# DirectAccess Setup Wizard-Step 1

- Security groups for DirectAccess clients



# DirectAccess Setup Wizard-Step 2

- Internet and intranet interfaces
- Smart card authorization

**DirectAccess Setup**

### DirectAccess Server Setup

A DirectAccess server provides connectivity and security to remote clients that securely access the internal network.

**Connectivity**

Certificate Components

In order to setup your DirectAccess server, you must select which interfaces connect to the Internet and the internal network. Please select the interfaces below.

Interface connected to the Internet: Internet (131.107.0.3) [Details...]

Interface connected to the internal network: Corpnet (10.0.0.2) [Details...]

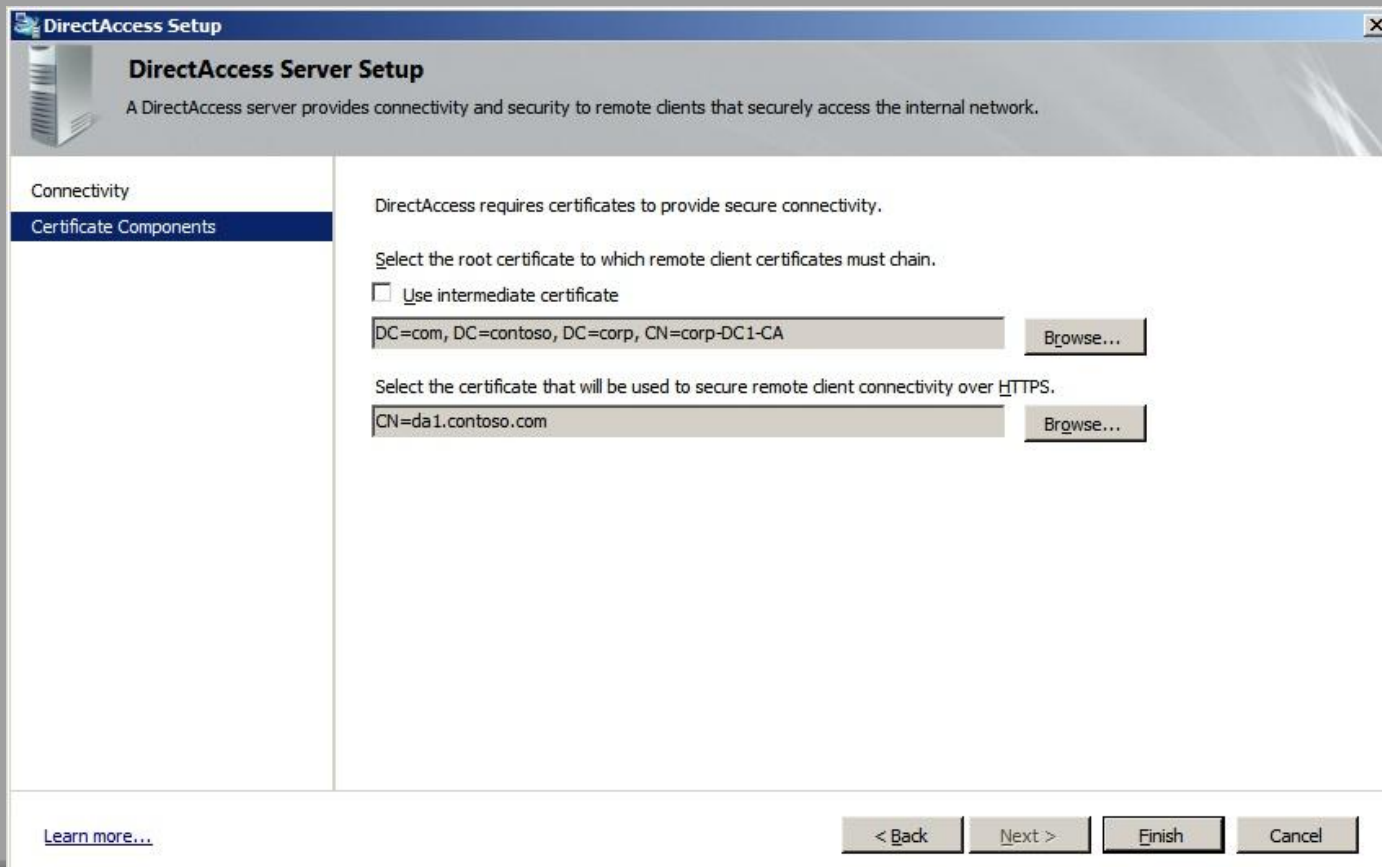
Require smart card login for remote users, and enforce this policy on the DirectAccess server

**i** To provide IPv6 connectivity over the existing IPv4 network, IPv6 transition technologies will be enabled on the DirectAccess server.

[Learn more...](#) < Back Next > Finish Cancel

# DirectAccess Setup Wizard-Step 2 (cont.)

- Certificate authentication for IPsec and the IP-HTTPS certificate



# DirectAccess Setup Wizard-Step 3

- Network location HTTPS URL

The screenshot shows the 'DirectAccess Setup' window, specifically the 'Infrastructure Server Setup' step. The window title is 'DirectAccess Setup' and it has a close button (X) in the top right corner. Below the title bar, there is a sub-header 'Infrastructure Server Setup' with an icon of server racks. A descriptive text reads: 'Remote client computers must be able to access infrastructure servers before they can connect to resources on the internal network. Please provide information about the infrastructure servers.'

The main content area is divided into two panes. The left pane, titled 'Location', contains a tree view with 'DNS and Domain Controller' and 'Management' under it. The right pane contains the following text: 'DirectAccess requires a highly available and scalable Network Location server. This server should be deployed with a server infrastructure such as domain controllers.'

There are two radio button options:

- Network Location server is run on a highly available server (recommended).  
Select the URL that will be used to provide clients with location information.  
A text box contains 'https://hls.corp.contoso.com' and a 'Validate' button is to its right.
- Network Location server is run on the DirectAccess server.  
The administrator will take the appropriate steps to ensure that the DirectAccess server is highly available.  
Select the certificate that will be used to secure location identification.  
A text box is empty and a 'Browse...' button is to its right.

A note at the bottom of the right pane states: 'Note: If the Network Location server is not available, connectivity may be disrupted.'

At the bottom of the window, there is a 'Learn more...' link on the left and four buttons on the right: '< Back', 'Next >', 'Finish', and 'Cancel'.

# DirectAccess Setup Wizard-Step 3 (cont.)

- NRPT rules

**DirectAccess Setup**

### Infrastructure Server Setup

Remote client computers must be able to access infrastructure servers before they can connect to resources on the internal network. Please provide information about the infrastructure servers.

Location

**DNS and Domain Controller**

Management

Enter the DNS suffixes and the IP addresses of the internal DNS servers (which are assumed to be running on domain controllers). Remote client computers will use this list of DNS suffixes to determine which DNS queries should be directed to the internal DNS servers.

Name Suffix	IPv6 address of DNS Server
corp.contoso.com	2002:836b:2:1:0:5efe:10.0.0.1
nls.corp.contoso.com	
*	

Select a local name resolution option:

- Only use local name resolution if the name does not exist in DNS (most restrictive)
- Fall back to local name resolution if the name does not exist in DNS or the DNS servers are unreachable when the client computer is on a private network (recommended)
- Fall back to local name resolution for any kind of DNS resolution error (least secure)

[Learn more...](#)

< Back   Next >   Finish   Cancel

# DirectAccess Setup Wizard-Step 3 (cont.)

- Identify management servers

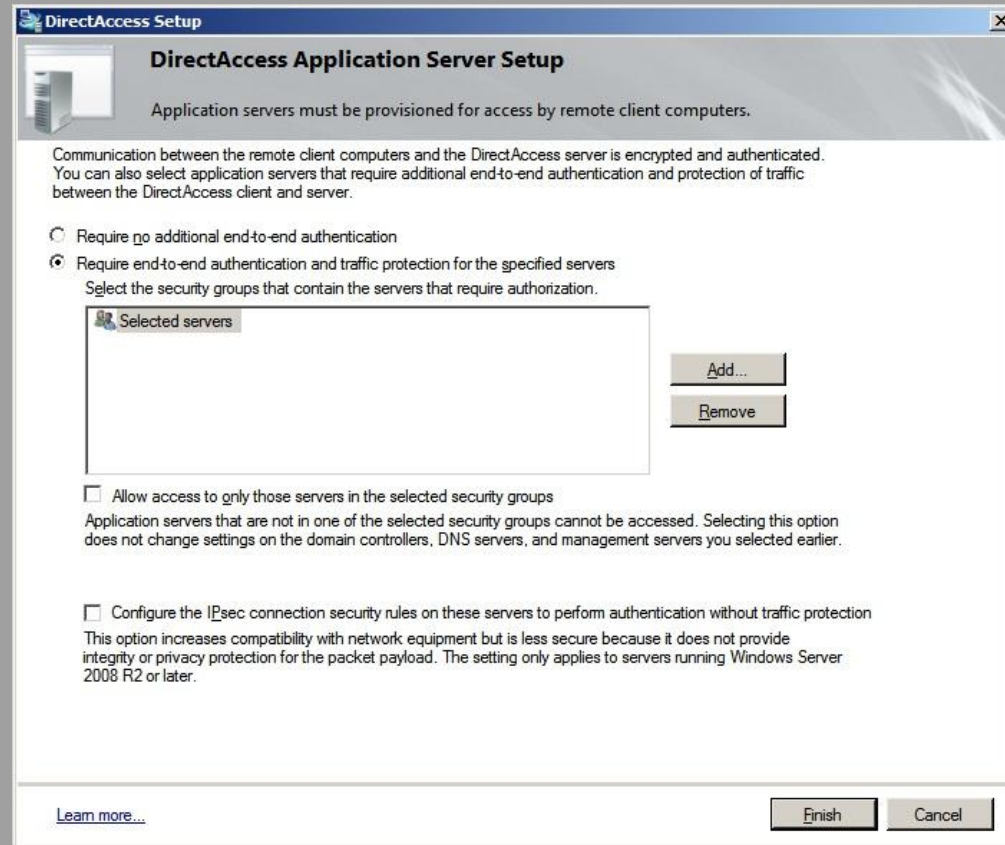
The screenshot shows the 'DirectAccess Setup' window, specifically the 'Infrastructure Server Setup' step. The window title is 'DirectAccess Setup' and the subtitle is 'Infrastructure Server Setup'. Below the subtitle, there is a note: 'Remote client computers must be able to access infrastructure servers before they can connect to resources on the internal network. Please provide information about the infrastructure servers.' On the left side, there is a navigation pane with three options: 'Location', 'DNS and Domain Controller', and 'Management', with 'Management' selected. The main area contains the text: 'Internal computers can manage remote client computers provisioned for DirectAccess. Enter the name or IP prefix of the management server(s) that will remotely manage DirectAccess clients.' Below this text is a table with the following content:

	IP Address/Prefix
▶	2002:836b:2:1:200:5efe:157.60.79.2
*	

At the bottom of the window, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. There is also a 'Learn more...' link in the bottom left corner.

# DirectAccess Setup Wizard-Step 4

- Selected server access model
  - End-to-end protection and exclusive access to selected servers
  - End-to-end protection to selected servers and no protection to all other servers



# Result of DirectAccess Setup Wizard

TechNet Events

- DirectAccess client GPO
  - IPv6 transition technologies
  - Connection security rules
  - NRPT entries
  - Intranet detection settings
- DirectAccess server GPO
  - Connection security rules
- Selected servers GPO
  - Connection security rules

# Result of DirectAccess Setup Wizard (cont.)

- DirectAccess server configured as
  - 6to4 relay
  - Teredo server and relay
  - IP-HTTPS server
  - ISATAP router

# DirectAccess Deployment Options

- High availability
  - Hyper-V configuration
- Scaling up
  - Microsoft Forefront Unified Access Gateway (UAG) (in beta)
    - Includes a NAT64
- Network Access Protection (NAP) integration
  - Require health certificates for intranet tunnel
- Server and domain isolation integration

# DirectAccess Deployment Options (cont.)

- Moving IPsec gateway function to another computer with IPsec offload hardware
- Force tunneling
- Providing DirectAccess clients access to the IPv6 Internet

# Using DirectAccess and VPN Concurrently

- Configure VPN servers to allow access to network location server, even when access is restricted
- Must use separate VPN and DirectAccess servers
  - UAG allows them to coexist on the same server
- Client is either using VPN connection or DirectAccess
  - When VPN connection is active, computer is on the intranet and DirectAccess is not used
  - When VPN connection is not active, computer is not on the intranet and DirectAccess is used

- DirectAccess
  - [DirectAccess Solution Web site](#)
  - [DirectAccess TechNet Web site](#)
  
  - [DirectAccess Design Guide](#)
  - [DirectAccess Deployment Guide](#)
  - [DirectAccess Troubleshooting Guide](#)
  
  - [Step By Step Guide: Demonstrate DirectAccess in a Test Lab](#)
- IPv6
  - [Understanding IPv6, 2<sup>nd</sup> Edition MS Press book](#)

**Microsoft®**

*Your potential. Our passion.™*