Microsoft® | Services

DirectAccess in Windows 7 and
Windows Server 2008 R2

Aydin Aslaner
Senior Support Escalation Engineer
Microsoft MEA Networking Team

Introduction to DirectAccess

Increasingly, people envision a world of anywhere access - a world in which the information, the communities, and the content that they value is available instantly and easily, no matter where they are.

Bill Gates

Enabling Secure Anywhere Access in a Connected World, Feb 2007
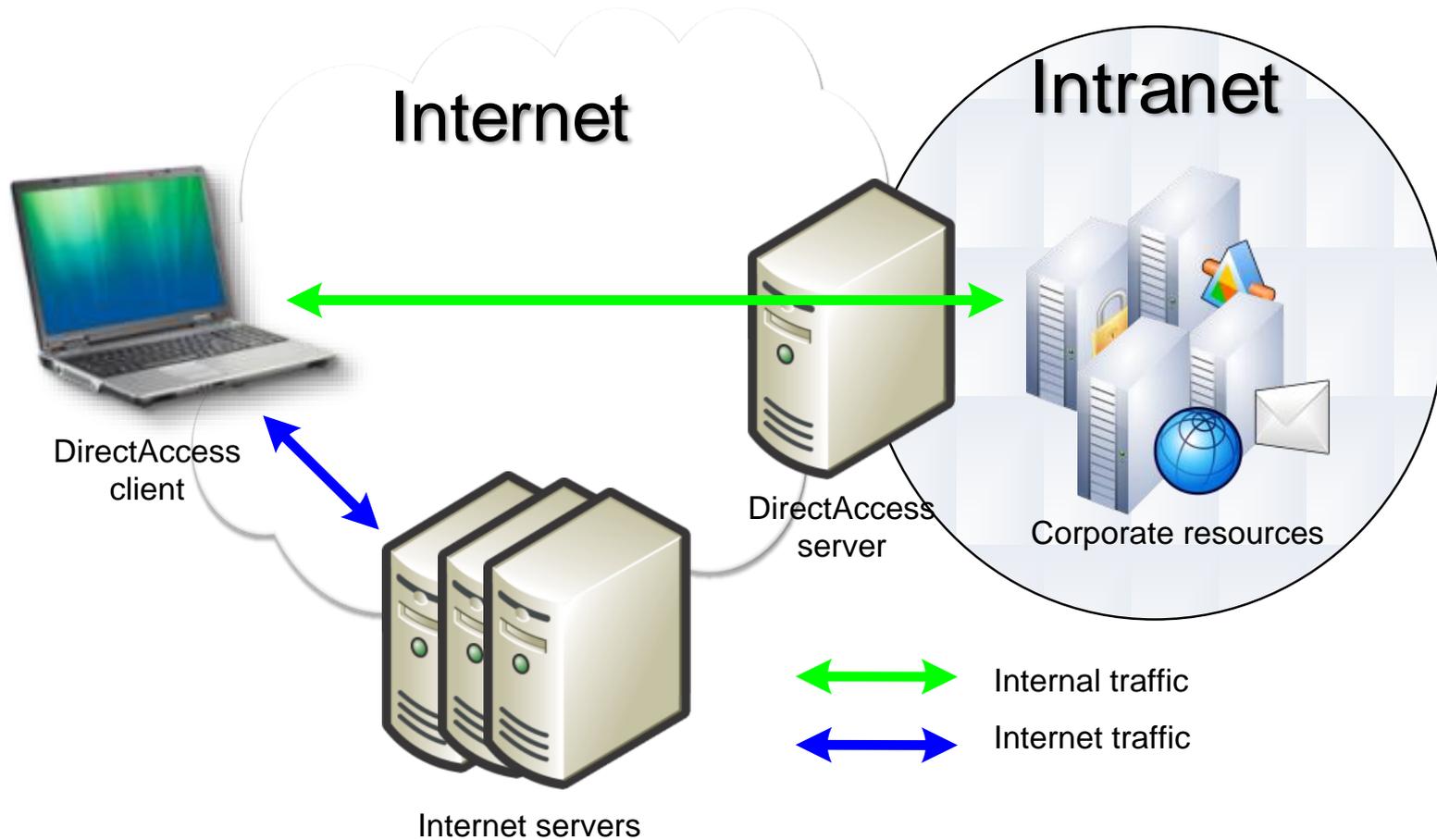
Microsoft | Services

Introduction
DirectAccess

- Remote user connects to Internet
  - User is directly connected to corporate network
    - Allows user to have their usual corporate access
  - Corporate network is directly connected to user
    - Allows management, patching, etc
- User doesn't have *to do* anything
  - Traditional VPNs require user to *bring up* the VPN
- User can maintain their local resource access
  - Connectivity to corporate network secured from local network/Internet
  - Traditional VPN often *disconnects* local resources
    - Sometimes deliberate for security – sometimes no choice
- Administrators *can* restrict/remove local access if needed

Introduction

Internet

Intranet

DirectAccess
client

Internet servers

DirectAccess
server

Corporate resources

Internal traffic

Internet traffic

Microsoft | Services

Introduction
Benefits of DirectAccess

- Always-on connectivity
- Seamless connectivity
- Bidirectional access
- Improved security
- Integrated solution

Part 2: Connectivity

This module explains how DirectAccess clients can maintain constant connectivity to the Internet whilst simultaneously accessing internal corporate resources (if required). It introduces the IPv6 transition technologies required to support DirectAccess.

Microsoft | Services

IPv6
Why IPv6?

- Virtually unlimited addresses
- Split Tunnel

    A scenario in which a machine can maintain connectivity to one network whilst tunneling to another.

    - Difficult to configure in IPv4 environments where many networks share IP addresses
    - Often disliked for security reasons
        - Can be configured securely

- Point-to-point security
    - NAT technology (needed to overcome IPv4 address shortage) *breaks* point-to-point address security
    - IPv6 does not need NATs

IPv6
IPv6 Transition Technologies

- 3 transition technologies to support IPv6 tunneling through IPv4 networks
  - 6to4
    - Router to router
    - IPv4 addresses of routers are embedded in IPv6 address
  - Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
    - Host to host tunnels
    - IPv4 addresses of hosts are embedded in IPv6 host address
  - Teredo
    - Host to host tunneling in UDP
    - IPv4 addresses of host NAT and supporting Teredo server embedded in IPv6 address
    - Provides automatic IPv4 NAT traversal

External Connectivity

If the client is assigned a:	Preferred connectivity method:
Globally routable IPv6 address	Globally routable IPv6 address
Public IPv4 address	6to4
Private (NAT) IPv4 address	Teredo
If the client cannot connect using the above	IP-HTTPS

IPv6
IP-HTTPS

- New protocol for Windows 7/Windows Server 2008 R2
- Tunnels IPv6 inside an IPv4-based HTTPS session
- Performance is not as good as other DirectAccess connection protocols
- Performance can be improved by:
  - Adding additional HTTPS servers and load balancing
  - Disabling IPsec encryption between DirectAccess client and DirectAccess server
- Microsoft is investigating further ways to improve performance of this technology

Intranet Connectivity

- DirectAccess needs resources to be reachable with IPv6
- Three ways to achieve intranet IPv6 connectivity
    - Support native IPv6
    - Deploy ISATAP
    - Use Network Address Translation - Protocol Translation (NAT-PT)

Intranet Connectivity
ISATAP

- RFC 4214

- Transition technology
    - Provides IPv6 connectivity between IPv6/IPv4 hosts across an IPv4-only intranet
    - Used for DirectAccess to ISATAP hosts on your intranet
    - ISATAP addresses displayed with last 32 bits in dotted decimal format
        - Highlights IPv4 address from which they are derived
          ```
          2001:101:102:1:0:5efe:172.20.77.15
          ```

Intranet Connectivity
NAT-PT

- RFC 2766

- Provides DirectAccess to IPv4-only resources on an intranet

- Currently, no NAT-PT implementation in Windows Server 2008 R2

  - NAT-PT devices available from Layer 2 switch and Layer 3 router vendors

  - Microsoft has released a NAT-PT implementation as part of a UAG Server

Name Resolution Policy Table and DNS
NRPT

- New feature for Windows 7/Windows Server 2008 R2
  - DNS servers can be defined per DNS namespace rather than per interface.
  - DNS queries for specific namespaces can be optionally secured using IPsec (and other actions can be specified)
- Helps separate Internet traffic from intranet traffic
- NRPT stores a list of DNS namespaces and configuration settings
  - Specifies DNS client behavior for each namespace
- When a DA client detects it is remote, it uses the NRPT to determine its DNS behavior

Name Resolution Policy Table and DNS
NRPT - Exemption Policies

- Some names need to be treated differently from others for name resolution
  - These names must *not* be resolved from the *internal* DNS server
- These servers' addresses must *always* be resolved from Internet DNS servers
  - WPAD servers
  - Inside/Outside servers
  - All quarantine servers

Part 3: IPsec

This module explains why an organization would choose to use IPsec to protect against attacks on their data and to provide end-to-end security, especially for clients using the DirectAccess feature of Windows.

It includes details on how to protect data with IPsec and how to plan your security.

IPsec

- Standards for ensuring secure communications over IP
- Defined by RFCs
- Can be used in 2 modes
  - Transport mode
    - IP Sec is applied directly to IP datagram
  - Tunnel mode
    - IP datagram is embedded as data within IPsec protected datagram
- DirectAccess uses IPsec policies for authentication and encryption of DirectAccess connections

Encryption

- When a DirectAccess client sends data, Internet traffic *should* be encrypted

- DirectAccess client computers may require domain access or remote management before the user logs on so computer authentication is required

- DirectAccess Clients have an IPsec policy which defines multiple rules

  1. Computer certificate based IPsec encryption with ESP
     Computer communicating with Intranet resources and vice versa
  2. User kerberos authentication and computer certificate
     Secure communications after the user has logged on

- IPsec sessions from DirectAccess client are terminated at an IPsec Gateway on DirectAccess server or stand-alone server

Authentication

- In order for the DirectAccess client to protect data, authentication is also required

- You can specify authentication without encryption

  - To mitigate spoofing/man-in-the-middle attacks

  - Use other data protection when sensitive data is transmitted with "*authentication-only*"

- DirectAccess accomplishes authentication by requiring ESP-NULL or Authentication Header (AH) for IPsec-protected communications

Microsoft | Services

Part 4: Requirements and Prerequisites

Before deploying DirectAccess, make sure that your environment meets all of the hardware, infrastructure, and network requirements listed in this lesson.

Microsoft | Services

Configuration Requirements
DirectAccess Server

- The DirectAccess server has the following requirements:
  - Joined to an Active Directory domain
  - Running Windows Server 2008 R2
  - Have at least two physical network adapters installed
  - Have at least two IPv4 addresses
    - Consecutive
    - Publicly addressable
    - Static
    - Externally resolvable through Internet DNS
- More than one DirectAccess server may be needed depending on deployment and scalability requirements

Configuration Requirements
DirectAccess Client

- DirectAccess clients have the following requirements:
  - Joined to an Active Directory domain
  - Running Windows 7 Ultimate or Enterprise Edition

    Clients not joined to an Active Directory domain or clients running Windows Vista or earlier versions of Windows are not supported

Infrastructure Requirements and Considerations

- Active Directory
  - At least one domain
- Group Policy
  - Recommended for centralized administration
- Domain controller
  - At least one DC running Windows Server 2008 or later
- Public key infrastructure (PKI)
  - For computer certificates
  - Public CRL required
- IPsec policies
  - As part of Windows Firewall with Advanced Security
- IPv6 and transition technologies
  - ISATAP, Teredo and/or 6to4

Part 5: Additional Deployment Options and Considerations

This module introduces additional DirectAccess deployment options such as ISATAP and Smart Card support.

It also includes a description of the remote management of DirectAccess and how to enable or disable connections between DirectAccess clients.

Deploying and Configuring
NRPT Configuration Example

- For client computers joined to **asia.contoso.com**

Suffix	Server
asia.contoso.com	asia_dns1 asia_dns2 asia_dns3

- For client computers joined to **europe.contoso.com**:

Suffix	Server
europe.contoso.com	europe_dns1 europe_dns2 europe_dns3

Smart Card Enforcement

- Smart card authentication for the IPsec Gateway, enforced when remote
  - Allows the user to logon to the computer and access the Internet without using a Smart Card
  - But Smart Card *required* for intranet access

Force Tunneling

- By default, remote DirectAccess clients are able to access
  - The Internet
  - The intranet
  - Their local subnet
  - This is technically a split tunnel scenario
    - Some administrators may not like this for security reasons
      - Although the per interface firewall rules may overcome this objection
- Force Tunneling
  - All client traffic is routed via IP-HTTPS to the intranet
    - Except local subnet e.g. a printer
  - Can be enabled by Group Policy
  - Only possible with IP-HTTPS

Publicly Available Names

- If DirectAccess policies use server names they must be publicly resolvable
- The following servers are usually in the policies
  - Teredo relay
  - 6to4 Relay
  - IP-HTTPS
  - May all be physically located on same server requiring only one name
- Policies can be configured using IP addresses for these servers

Microsoft | Services

Part 6: Designing a DirectAccess Solution

DirectAccess is a very flexible solution that can be deployed in different ways to meet customer requirements. Many decisions must be made in advance to ensure that DirectAccess design meets the needs of that environment. This lesson breaks down the numerous steps into smaller decision points to help you understand the big picture and make informed decisions.

Microsoft | Services

Where Do I Start?

- There are three main steps for designing a DirectAccess deployment:
  - Choose an access model
  - Choose a scalability model
  - Choose a deployment method

Design Influencers

- IPv6 and IPsec are the two key factors
  - IPv6
    - Only IPv6-enabled resources are accessible to DirectAccess clients
    - The only way to access IPv4-only resources is to use a NAT-PT device
  - IPsec
    - Provides a flexible framework for secure access in any requirement

- Windows Server 2008 supports use of IPsec connections with IPv6
- Windows Server 2003 and earlier versions of Windows Server do not fully support the use of IPsec with IPv6
  - IPv6-enabled resources on Windows Server 2003 will only be available to DirectAccess clients if you terminate IPsec with ESP+Encryption at the edge of the network (the end-to-edge access model)

Choosing an Access Model

- There are three access models to choose from:
    - Full intranet access (end-to-edge)
    - Selected server access (modified end-to-edge)
    - End-to-end

Choosing an Access Model
Full Intranet Access (End-to-Edge)

- Allows DirectAccess clients to connect to all intranet resources
- Uses IPsec tunnel policies requiring
    - authentication
    - encryption
    - Termination at IPsec Gateway
- By default, the IPsec Gateway is hosted on the DirectAccess server but can be moved
- Works with application servers running Windows Server 2003 and above
    - IPsec-protected traffic is kept off of the intranet
    - Similar to current VPN architecture → might be easier to deploy in short term

Choosing an Access Model
Selected Server Access (Modified End-to-Edge)

- Very similar to the Full Intranet access model with one addition
  - ESP+NULL or AH are used to authenticate traffic from the client to the application server
  - Client communications are still encrypted to the IPsec Gateway
  - Maintains a high degree of confidence that the client is communicating with the intended servers
- Authenticate only (Null Encapsulation) is a new policy available only on Windows Server 2008 R2
  - Provides IPsec authentication on the first packet
  - Does not provide per-packet integrity or privacy on subsequent packets
  - Traffic flows in the clear after the IKE session has been negotiated
- Networks that contain hardware that does not support IPsec-protected traffic might benefit from this solution

Choosing an Access Model
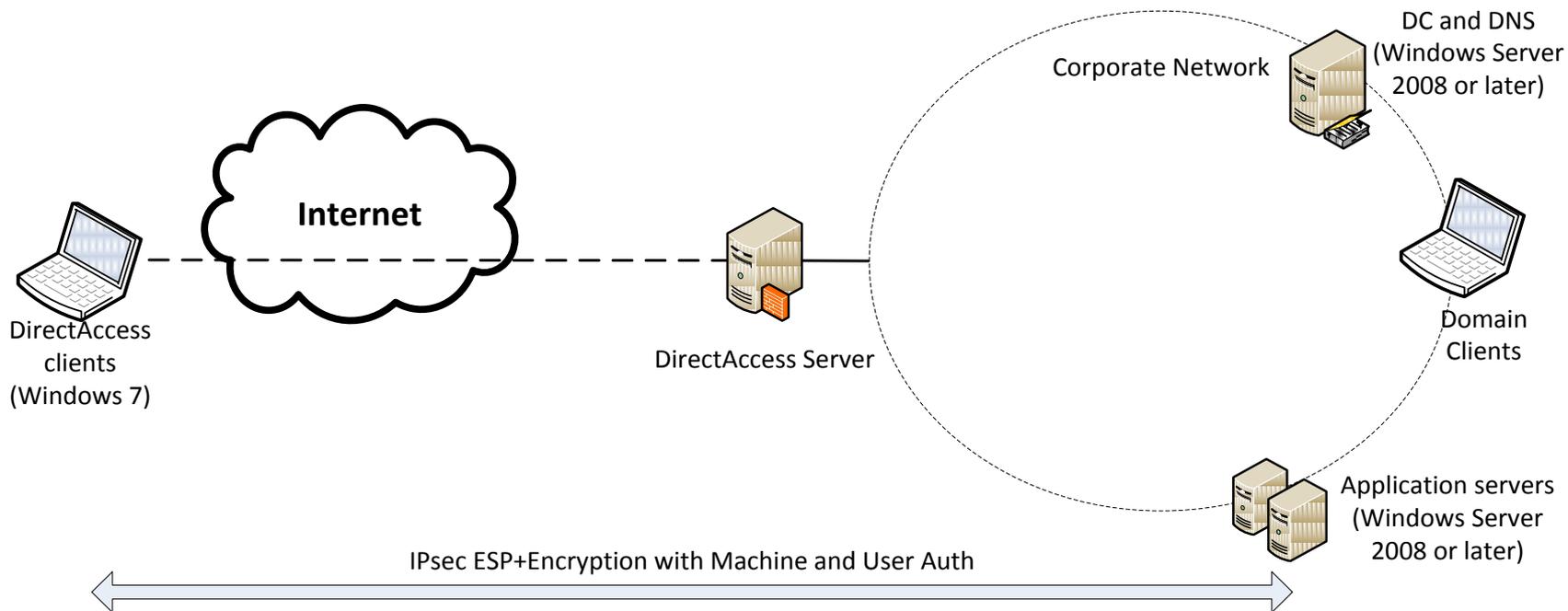## Selected Server Access (Modified End-to-Edge)

Internet

DirectAccess clients (Windows 7)

DirectAccess Server

Corporate Network

DC and DNS (Windows Server 2008 or later)

Domain Clients

Application servers (Windows Server 2008 or later)

IPsec ESP tunnel/IP-TLS encryption with Machine Auth (DC/DNS access)

IPsec ESP tunnel/IP-TLS encryption with Machine Auth and User Auth (App servers access)

IPsec ESP NULL (transport mode) with Machine Auth and User Auth (App servers access)
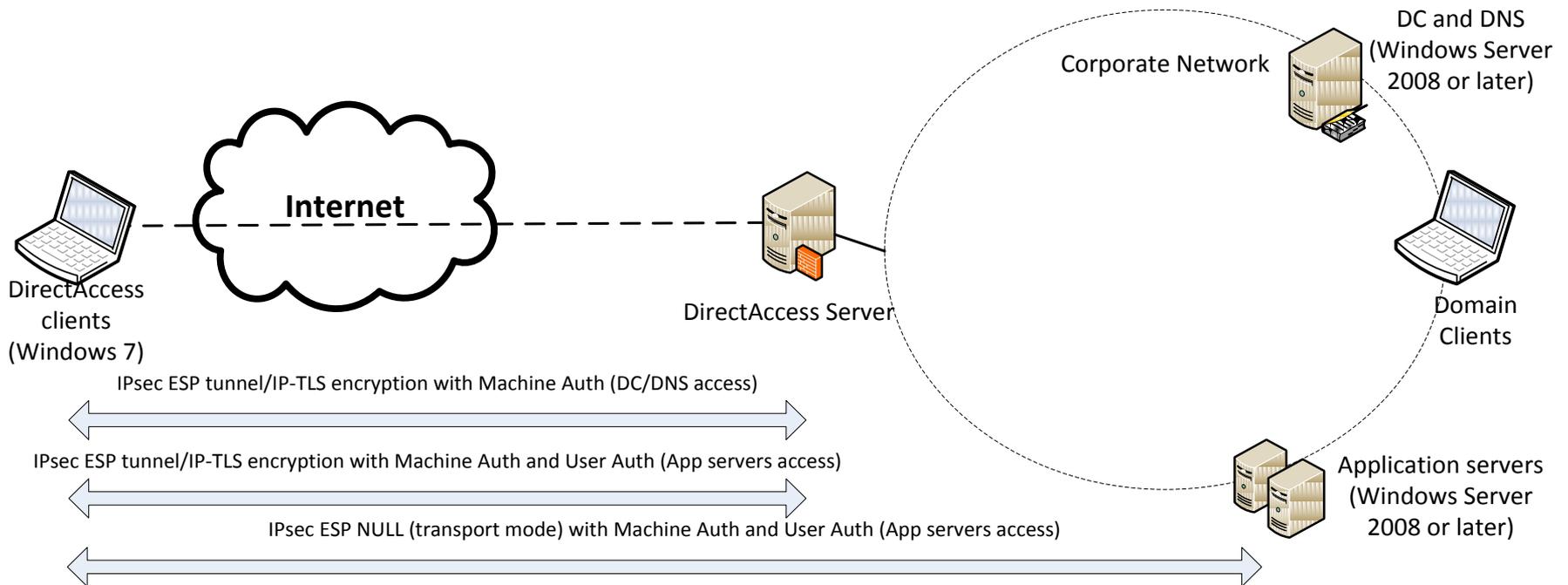
Choosing an Access Model
End-to-End

- Extends the full IPsec policies all the way to the application server
    - DirectAccess clients use IPsec transport policies that require encryption and authentication that terminate at the application servers
    - DirectAccess server/IPsec Gateway simply acts as a pass-through device
- This model makes it easier to create restriction policies to prevent specific users or applications from accessing specific servers

Choosing an Access Model
End-to-End

DC and DNS
(Windows Server
2008 or later)

Corporate Network

Internet

DirectAccess
clients
(Windows 7)

DirectAccess Server

Domain
Clients

Application servers
(Windows Server
2008 or later)

IPsec ESP+Encryption with Machine and User Auth

Microsoft | Services

Choosing a Scalability Model
Single Server
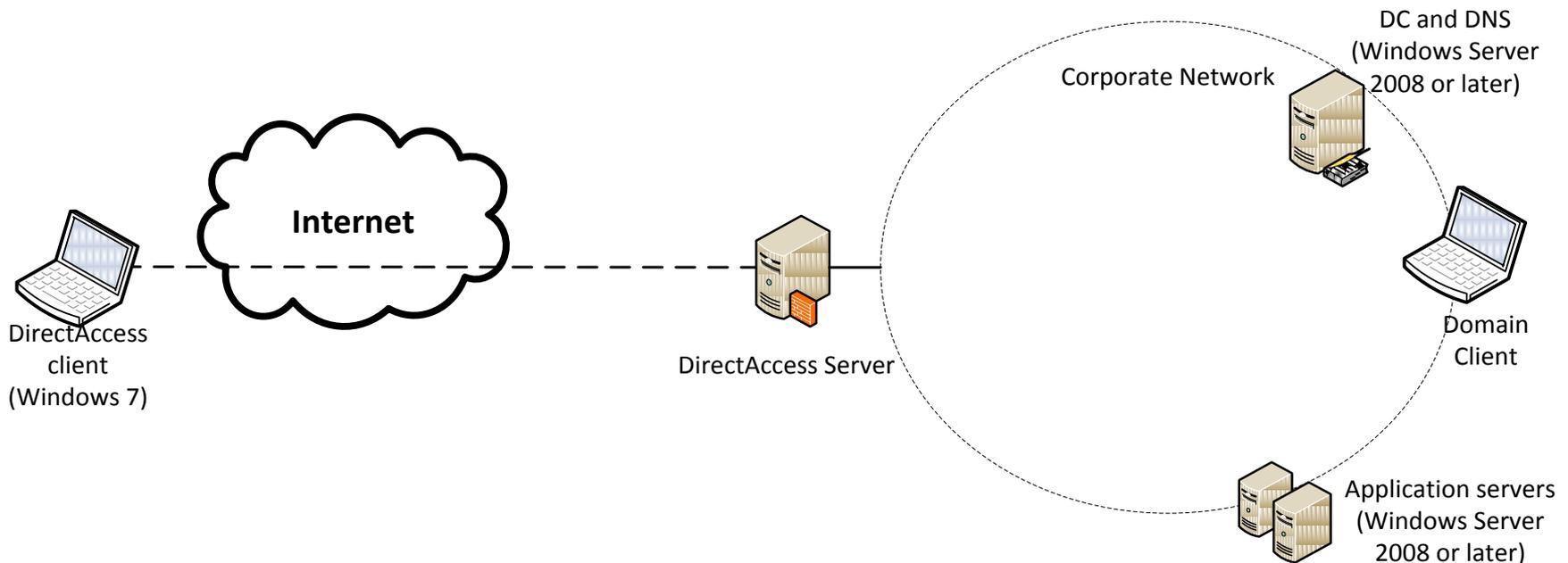
Choosing a Scalability Model
Multiple Servers for High Availability
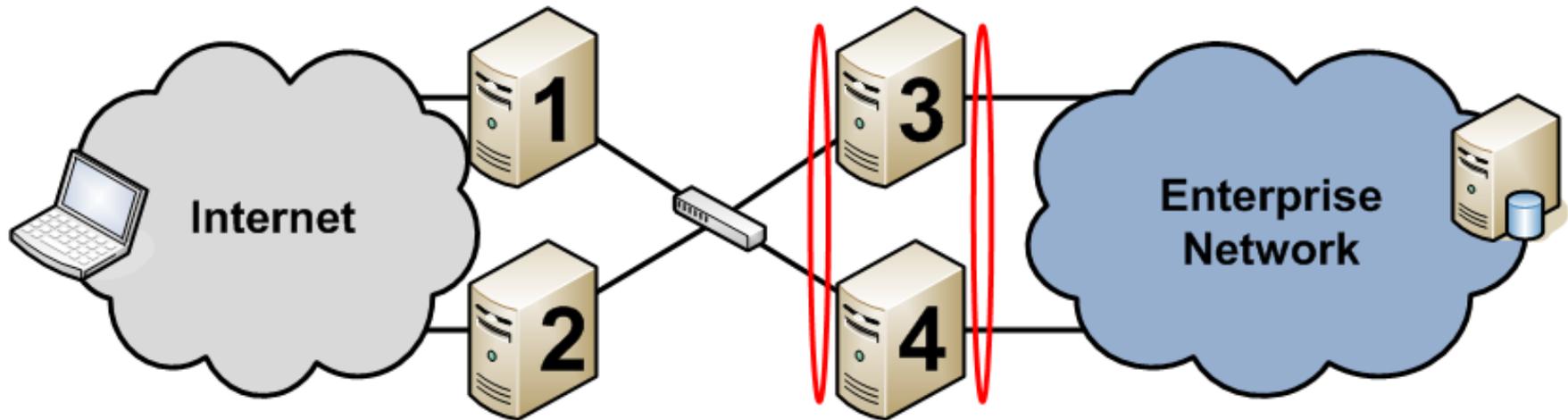
- Servers 1 & 2 are configured with Teredo server/Teredo Relay/6to4 Relay and IP-HTTPS servers
- Servers 3 & 4 are configured with the IPsec Gateway and a Network Load Balancer
- Bi-directional routing between 1 & 2 and 3 & 4

Choosing a Deployment Method

- You can use the following methods to deploy and configure DirectAccess resources:
    - The DirectAccess Management Console
    - Scripted installation using Netsh.exe
    - Client configuration using Group Policy

Part 7: DirectAccess Monitoring

Windows Server 2008 R2 provides built-in monitoring of the DirectAccess server and its components through the DirectAccess Monitoring snap-in. The DirectAccess Monitoring snap-in provides the ability to monitor traffic activity, data, and control traffic counters and events for the different components of the DirectAccess server and system status of the DirectAccess server.

Microsoft | Services

DirectAccess Server Status

- DirectAccess server status updated every 10 seconds
- If any component reports a Warning state (in yellow), the system state also reports a Warning
- If any component reports an Error state (in red), the system state also reports an Error
- If both Warning and Error states are reported, the system state shows an Error (in red)
- Errors and Warnings will be accompanied with suggested remediation

DirectAccess Server Status

DirectAccess Server Status
DirectAccess Server Components

- Shows status of the following components:
  - Teredo Relay,
  - Teredo server
  - 6to4 gateway
  - ISATAP
  - IP-HTTPS
  - Network Security
  - DNS servers
- Provides "*Details*" buttons for each component (except DNS)
  - Launches Performance Monitor snap-in with preconfigured counters for the selected component
- Teredo Relay, Teredo Server, ISATAP and 6to4 display "*Healthy*" if there was any traffic in the last 10 seconds
- IP-HTTPS and Network Security display "*Healthy*" if there is at least one active session or tunnel
- No traffic (or active sessions) results in a yellow status
- If the component has failed or is under an attack, its status is red

DirectAccess Server Status
Management Pack

- Management pack for System Center Operations Manager (SCOM) SP1
  - Provides monitoring, threshold alarms, and report generation capabilities
- Set following registry value on each server to enable monitoring :
  ```
  HKEY_LOCAL_MACHINE\Software\Microsoft\DAServer\Management=1
  ```
- Displaying DirectAccess Server on SCOM Console
  - DirectAccess server displayed as parent and components displayed as child entities
  - For a scenario where components are spread across different computers, each computer is displayed as a DirectAccess server with enabled components under it

Troubleshooting
Additional Resources

Site	URL
Active Directory	http://www.microsoft.com/activedirectory
Clustering	http://www.microsoft.com/windowsserver2008/en/us/clustering-home.aspx
DNS	http://www.microsoft.com/dns
Group Policy	http://technet.microsoft.com/en-us/windowsserver/grouppolicy/default.aspx
IPv6	http://www.microsoft.com/ipv6
IPsec	http://www.microsoft.com/ipsec
NAP	http://www.microsoft.com/nap
PKI	http://www.microsoft.com/pki

Microsoft®

Your potential. Our passion.™