



Microsoft®

System Center

Summer Night

DirectAccess

Providing seamless, secure access to enterprise resources from and to anywhere

Ronny de Jong

Consultant

ronny.de.jong@inovativ.nl



#ronnydejong

inovativ 

..de System Center specialisten

Powered by:



Microsoft®
System Center

User Group **Netherlands**

Agenda

- ❖ Introduction
- ❖ End-User Experience
- ❖ Demo 1 – End User Experience
- ❖ Infrastructure Technologies
 - IPv6
 - Transition Technologies
 - Topology
 - Connectivity
 - Security
- ❖ Demo 2 – Security / Monitoring
- ❖ Summary
- ❖ Q&A

Introduction - What is Forefront UAG?

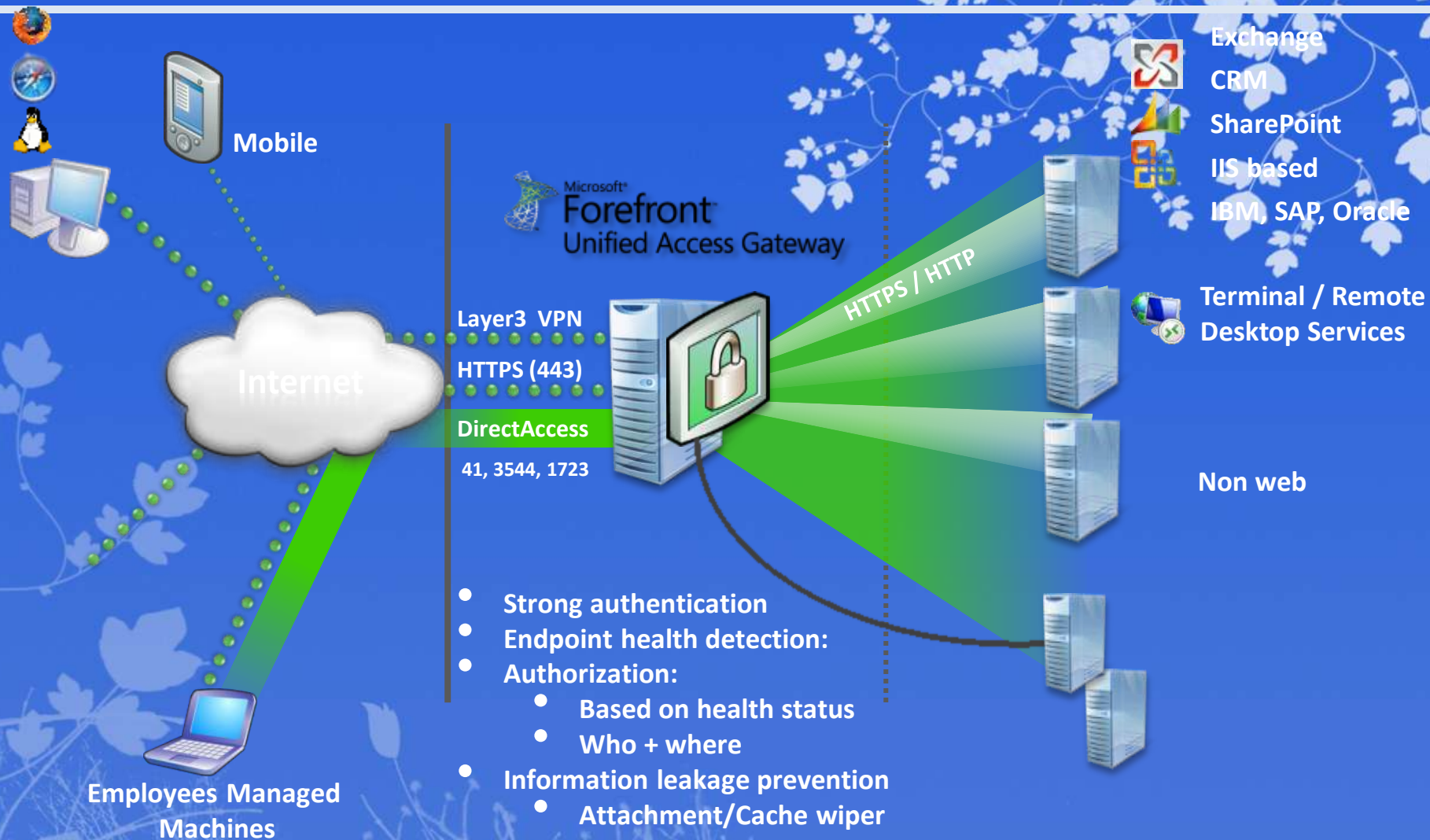
❖ Microsoft Forefront Unified Access Gateway

- Whale Communications Air Gap (acquired by MSFT 2006)
- Microsoft Intelligent Application Gateway (IAG) Server 2007
- Microsoft Unified Access Gateway (UAG) 2010

❖ UAG provides managed, unmanaged & mobile devices with unified secure anywhere access to on-premise and in-the-cloud applications.

- Web Publishing (Exchange, SharePoint, RemoteApps)
- Remote port and socket forwarding over an SSL tunnel
- Remote Desktop Gateway Publishing (RDG)
- SSL VPN
- DirectAccess

Introduction - UAG Solution Overview



Introduction - "Re-Perimeterization"

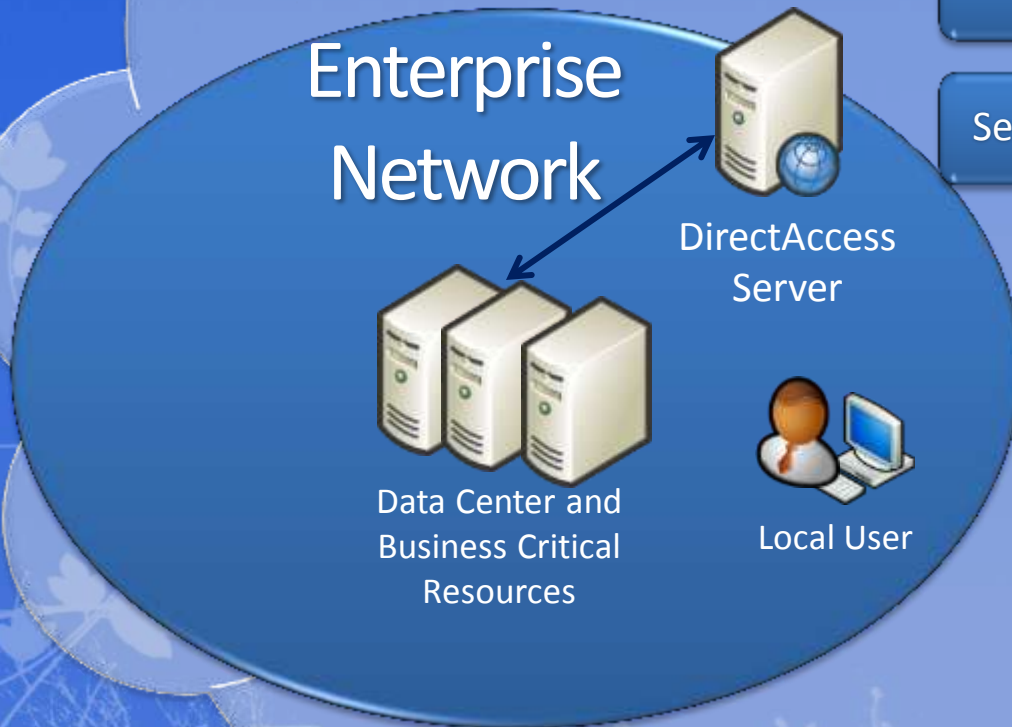
"My network is where my buildings are"



"My network is where my users and assets are"

- ❖ How to manage, monitor, and support remote users/machines all the time?
- ❖ How to simplify 'remote workers' access

Introduction - Industry Trends



Assume the underlying network is always unsecure

Redefine the corporate edge to protect the datacenter

Security policies based on identity, not location

Internet



Remote User



End-User Experience – Always ON

❖ Always ON – bidirectional connection

- Always connected
- No user action required
- Adapts to changing networks

❖ Makes “always managed” a reality

- Group Policy updates
- Software Deployment
- Backup
- Remote assistance initiated by IT
- Password changes CTRL+ALT+DEL



End-User Experience - Secure

❖ Secure

- Encrypted by default
- Works with Smartcards
- Granular access control
- Coexists with existing edge, health, and access policies



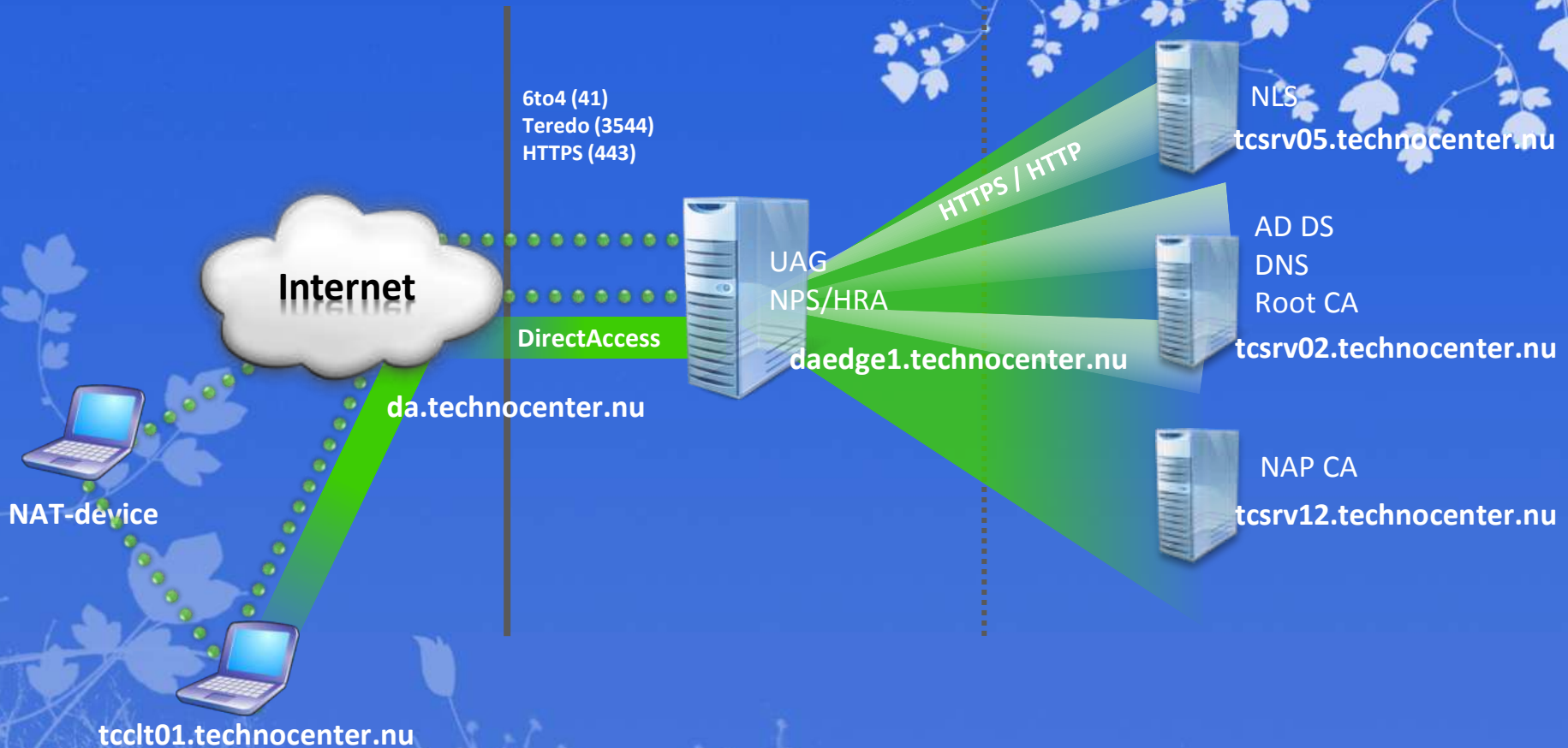
End-User Experience - Manageability



❖ Manageable

- Reach out to previously untouchable machines
- Allows remote clients to process Group Policies
- NAP integration for health compliance
- Consolidate Edge Infrastructure

Demo Configuration



Demo 1 – End-User Experience

Infrastructure Technologies

❖ Uses IPv6

- Solves IPv4 address depletion problem
- Window 7/2008+ transition technologies enable it over IPv4

Unique addresses (prevents the “hotel has the same network ID as the office” scenario)

```
Tunnel adapter Teredo Tunneling Pseudo-Interface:
Connection-specific DNS Suffix . : 
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:0:836b:b9:459:bc9d:b7bf:ab2d(Preferred)
Link-local IPv6 Address . . . . . : fe80::459:bc9d:b7bf:ab2d%16(Preferred)
Default Gateway . . . . . : 
NetBIOS over Tcpip. . . . . : Disabled

Tunnel adapter IPHTTPSInterface:
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft IP-HTTPS Platform Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
Dhcp Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:4898:c8:f013:6990:ea7:2862:6cc(Preferred)
Temporary IPv6 Address . . . . . : 2001:4898:c8:f013:fd70:1535:f8f8:358d(Preferred)
Link-local IPv6 Address . . . . . : fe80::6990:ea7:2862:6cc%19(Preferred)
Default Gateway . . . . . : 
NetBIOS over Tcpip. . . . . : Disabled
```

Infrastructure Technologies

❖ Getting IPv6 over the IPv4 Internet

- 6to4
- Teredo
- IP/HTTPS

❖ Getting IPv6 over the intranet

- NAT64
- ISATAP (Intra-site Automatic Tunnel Addressing Protocol)
- Native IPv6

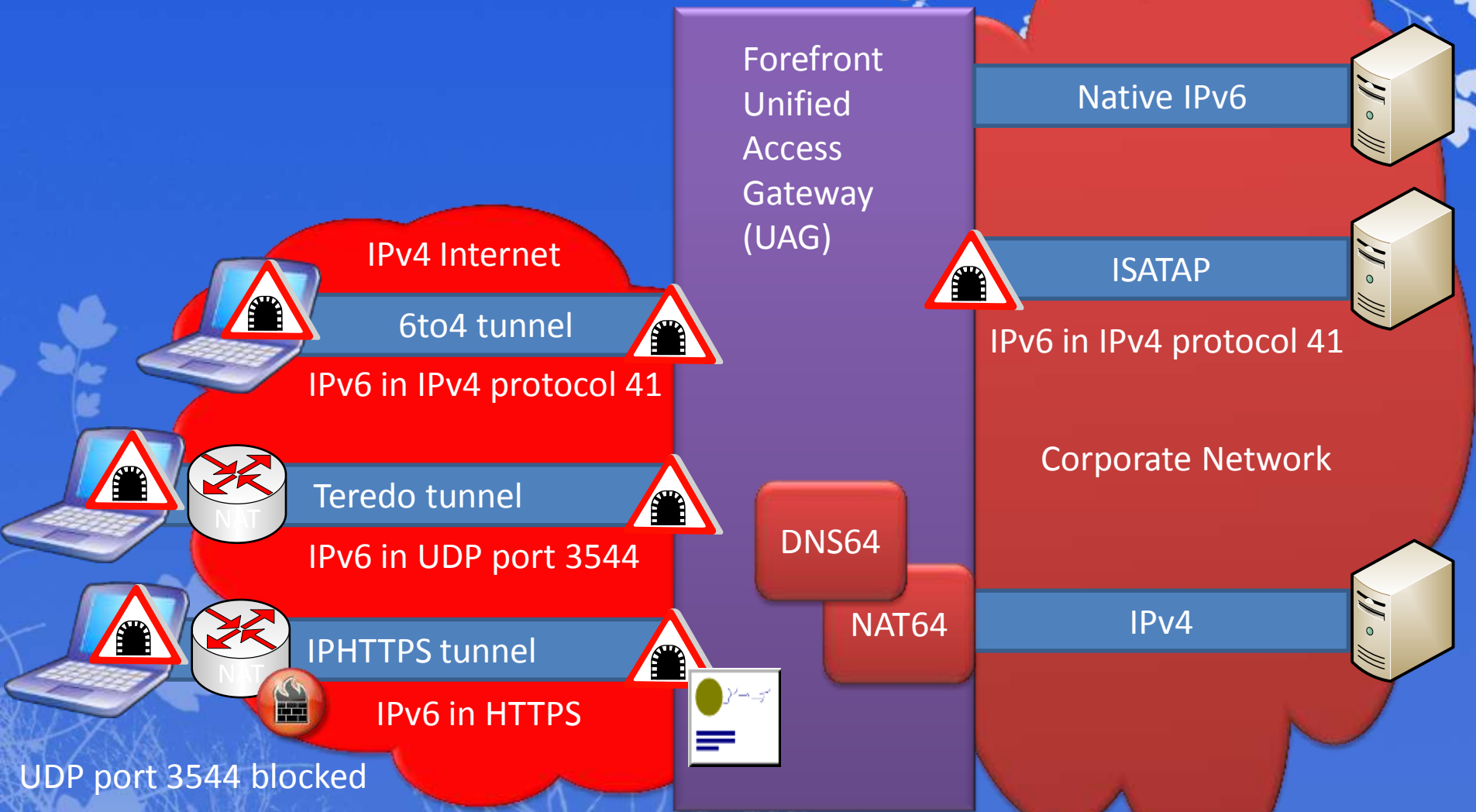


Infrastructure Technologies

- ❖ To be able to route traffic each network must have a different identity
- ❖ Teredo has a predefined network prefix of 2001::/32
- ❖ Wizard generates different networks based on the 1st 6to4 address of the Internet facing address

Network	Prefix
Network A: 6to4 (131.107.0.2)	2002:9013:c802:0000::/64
Network B: 6to4 (131.107.0.3)	2002:9013:c803:0000::/64
Network C: Teredo	2001:0::/32
Network D: IPHTTPS	2002:9013:c802:8100::/56
Network E: ISATAP	2002:9013:c802:8000::/64
Network F: NAT64	2002:9013:c802:8001:0000:0000::/96

Infrastructure Technologies



Infrastructure Technologies

Client side

	6to4	Teredo	IP-HTTPS
Transport	IP Protocol 41	UDP 3544	TCP 443
When is it used?	When client has <u>public</u> IPv4	When client is behind a NAT (<u>NAT assigned private address</u>)	Last resort
Server Side Component	6to4 Relay on the UAG	Teredo relay on the UAG	IP-HTTPS interface on the UAG

Infrastructure Technologies

Corporate side

	NAT64	ISATAP	Native
Transport	IPv4	IPv6 in IPv4 Protocol 41	IPv6
When would you want to use it?	Most cases	When you want to “touch” managed clients and don’t want to worry about IPv6 routes in your network.	In closed labs In Microsoft ☺ Organizations that adopted IPv6
Server Side Component	DNS64/NAT64	ISATAP Server installed if no Native IPv6	None
DNS Registration	Register as IPv4	Register as IPv6	Register as IPv6
Misc	<ul style="list-style-type: none">• RFC draft• Native and ISATAP get priority• Works perfectly with IPv4 stacks (for NAT friendly applications)• No reverse NAT• “Reduces” manage out	<ul style="list-style-type: none">• RFC 5214• Registers in the DNS• Vista+ 2008+• Can be applied only to specific servers• Direct Traffic between ISATAP hosts	<ul style="list-style-type: none">• Address assignment: Static, ICMP, DHCPv6

Deployment Configurations

❖ Access Model

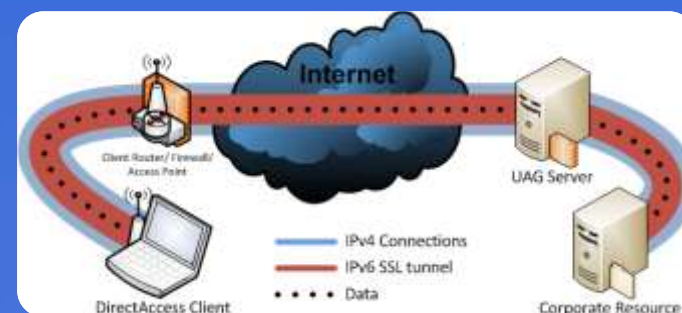
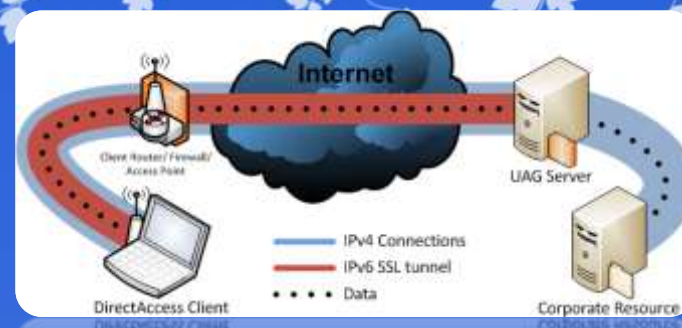
- ❖ End-to-Edge
- ❖ End-to-End

❖ Deployment Models

- ❖ Single Server
- ❖ Multiple Servers (Array)
- ❖ Multi Geo

❖ Deployment Models

- ❖ Full intranet Access
- ❖ Remote Management



End-to-edge encryption

Trusted, compliant,
healthy machine



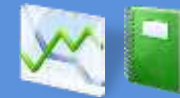
Internet

Direct Access
Server
Server 2008 R2



Corporate
Network

DC & DNS
(Server 2008 SP2/R2)



Applications & Data
(non-IPsec enabled)

Windows 7 client

IPsec ESP tunnel encryption using machine cert (DC/DNS access)

IPsec ESP tunnel encryption using UserKerb/Health
Cert/Smartcard for broad network access

Clear Text traffic from client flows through
encrypted tunnel to Corporate network resources

- ❖ No overhead of encryption on application servers
- ❖ Edge enforces machine/user authentication and data encryption
- ❖ Least change from customer's existing edge deployments

End-to-Edge Encryption + End to End IPsec

Trusted, compliant,
healthy machine



Internet

Direct Access
Server
Server 2008 R2



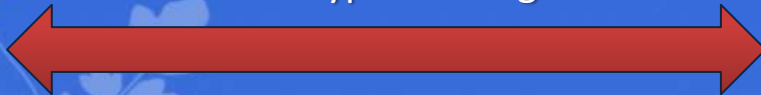
**Corporate
Network**
DC & DNS
(Server 2008 SP2/R2)



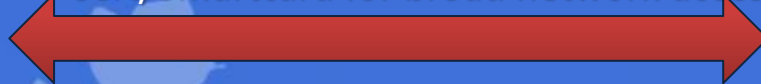
Applications & Data
IPsec-enabled

Windows 7 client

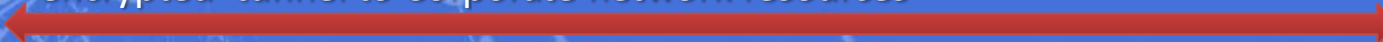
IPsec ESP tunnel encryption using machine cert (DC/DNS access)



IPsec ESP tunnel encryption using UserKerb/Health
Cert/Smartcard for broad network access



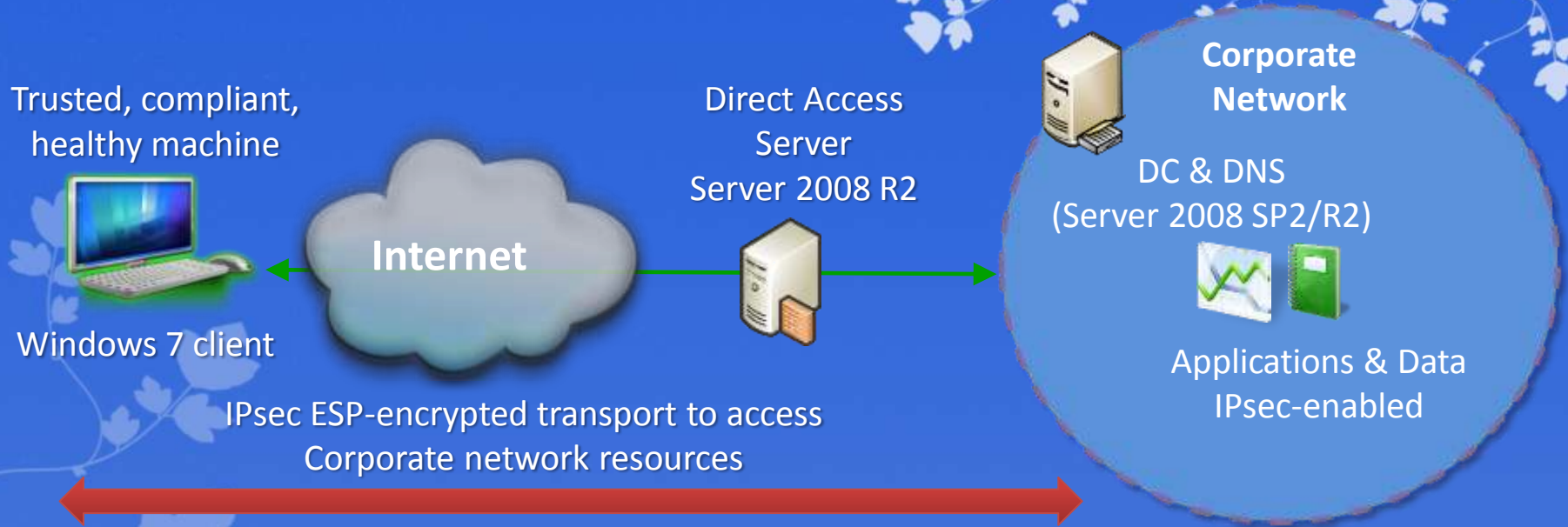
IPsec ESP-Null AuthIP Transport Traffic flows through
encrypted tunnel to Corporate network resources



- ❖ **No overhead of encryption on application servers (just authentication)**
- ❖ **DirectAccess Edge Encryption combined with End to End IPsec Server and Domain Isolation**



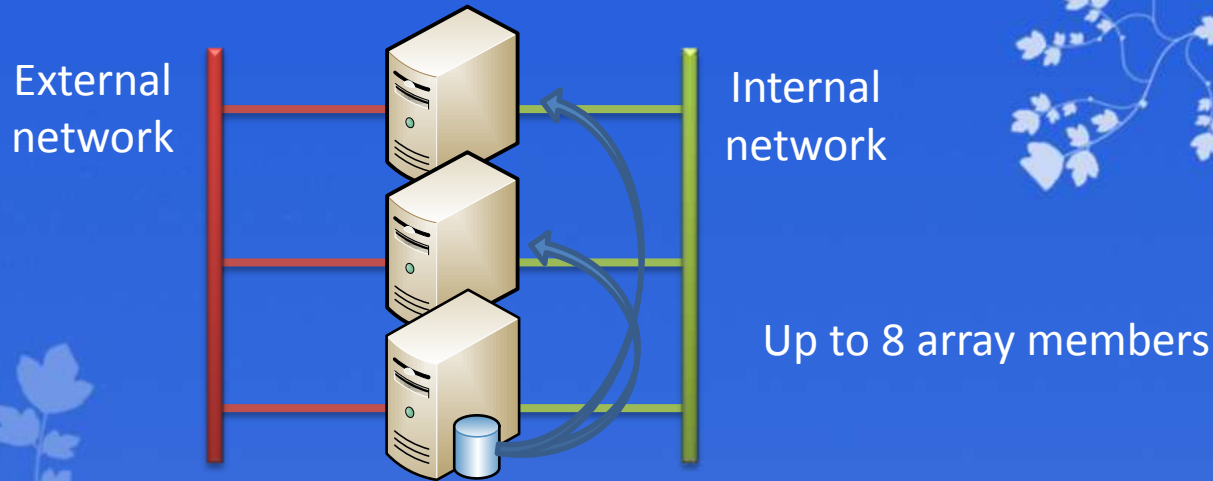
End-To-End IPsec Transport Encryption



IPsec ESP-encrypted transport to access Corporate network resources

- ❖ **Thin edge solution using IPsec**
- ❖ **Denial of Service Protection (DoSP) Service only allows Ipsec & ICMP traffic**
- ❖ **Full End to End IPsec Encryption**
- ❖ **IP-HTTPS tunnel used for proxy scenarios only**

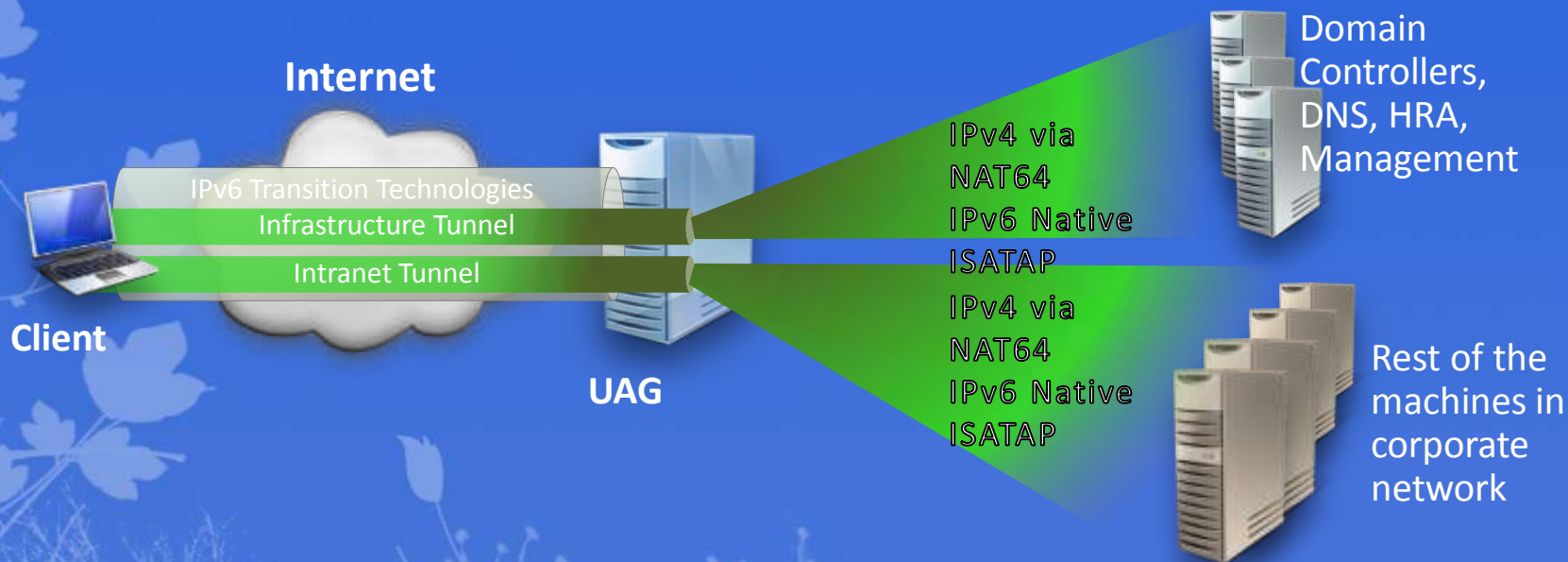
UAG Array



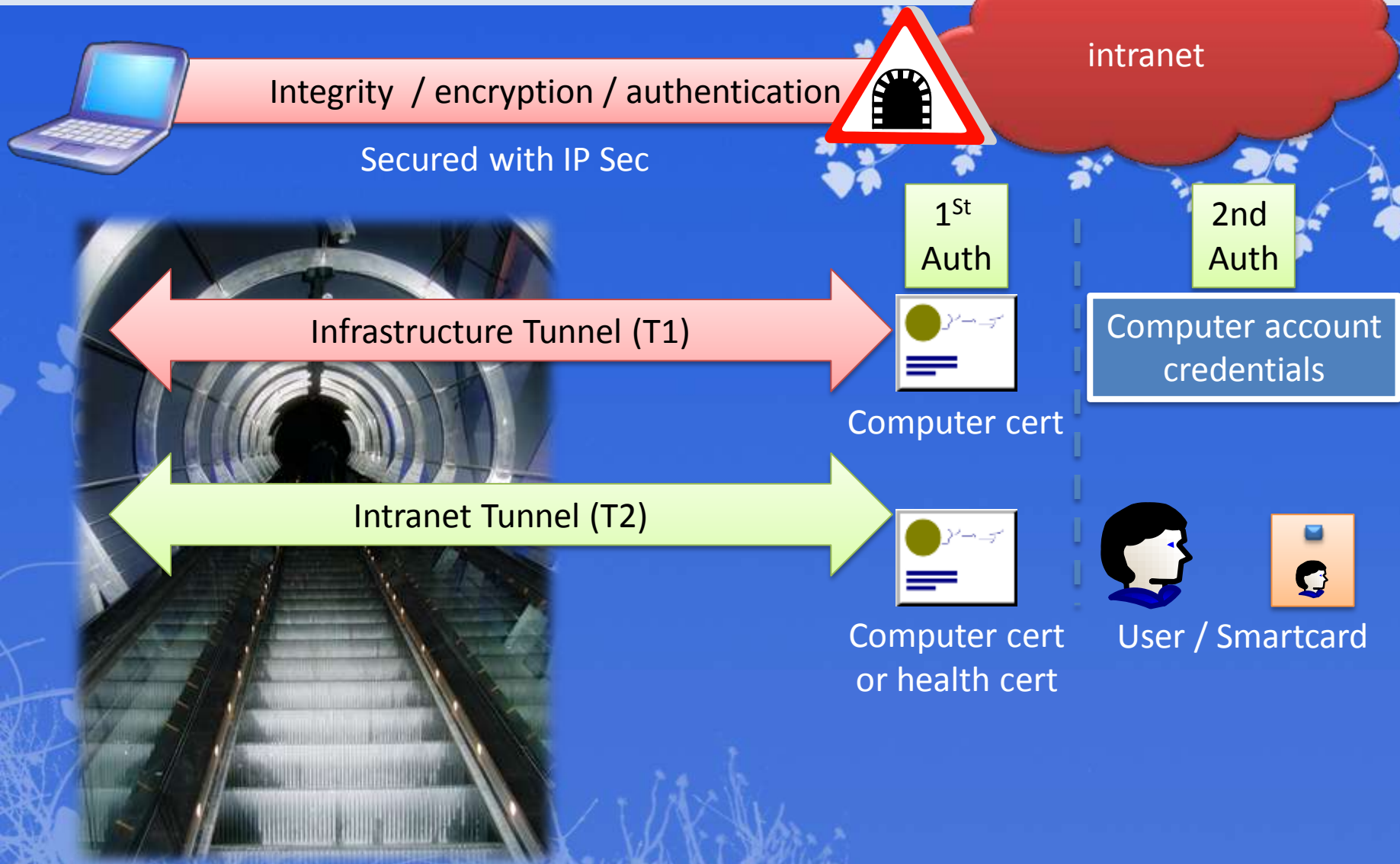
- ❖ **Array with Network Load Balancing (NLB) for increased scalability and availability**
- ❖ **One server acts as the Array Manager Server (AMS)**
 - Configuration automatically propagated to all other array members
 - Configuration stored in AD LDS
 - Up to 8 members per array

IPSec Tunnels

Connectivity to corporate network is done using IPv6, protected by IPSec tunnels and transported over IPv4 using IPv6 transition technologies (6to4, Teredo, IP-HTTPS):



Securing the Tunnels



Infrastructure Technologies - Requirements

❖ DirectAccess Client

- Windows 7 (Enterprise or Ultimate)
- Client Domain Joined

❖ DirectAccess Server

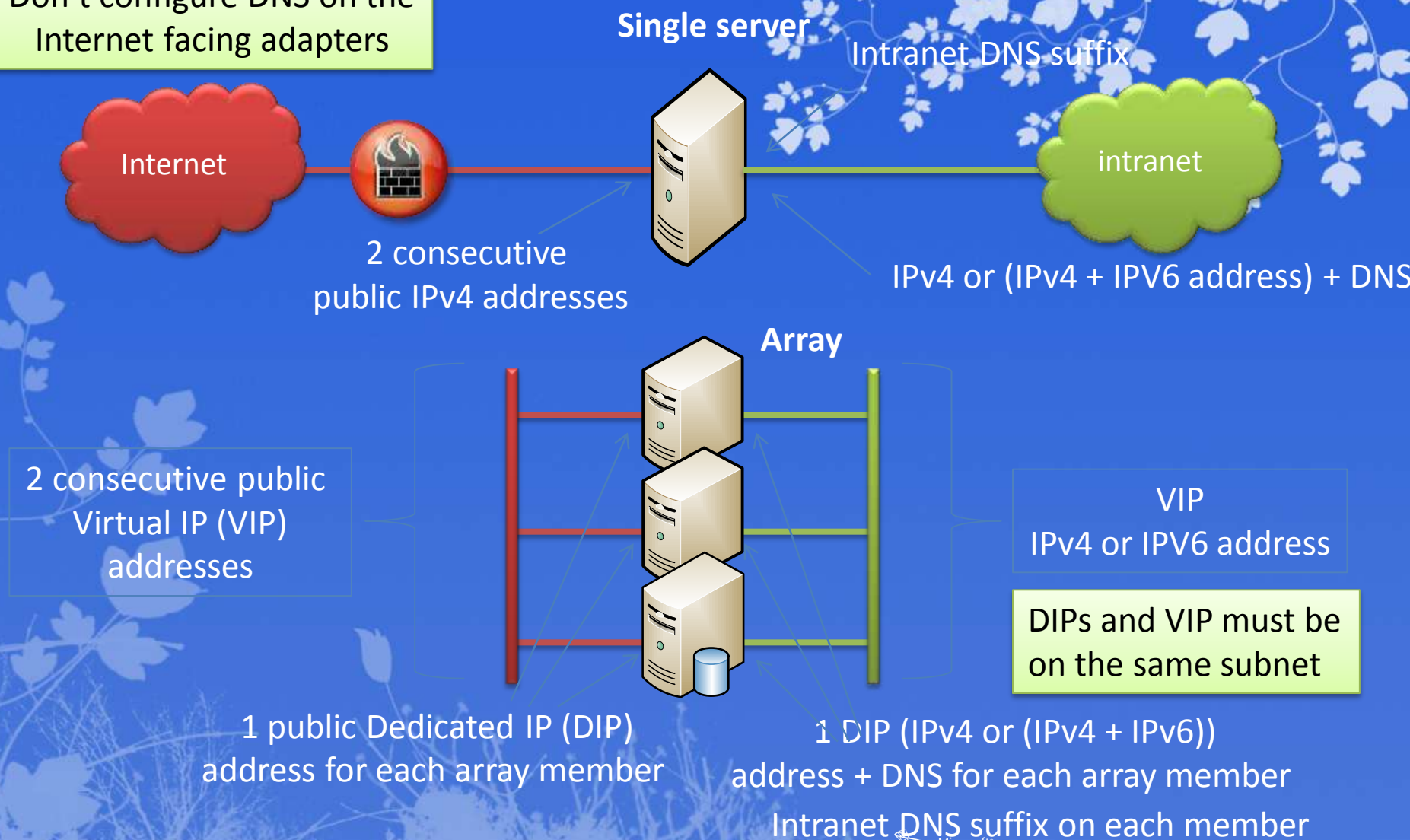
- Windows Server 2008 R2
- Forefront UAG 2010 SP1
- At least one W2K8 SP2 or R2 DC/DNS
- DirectAccess Client and Server are domain members

❖ Application Servers

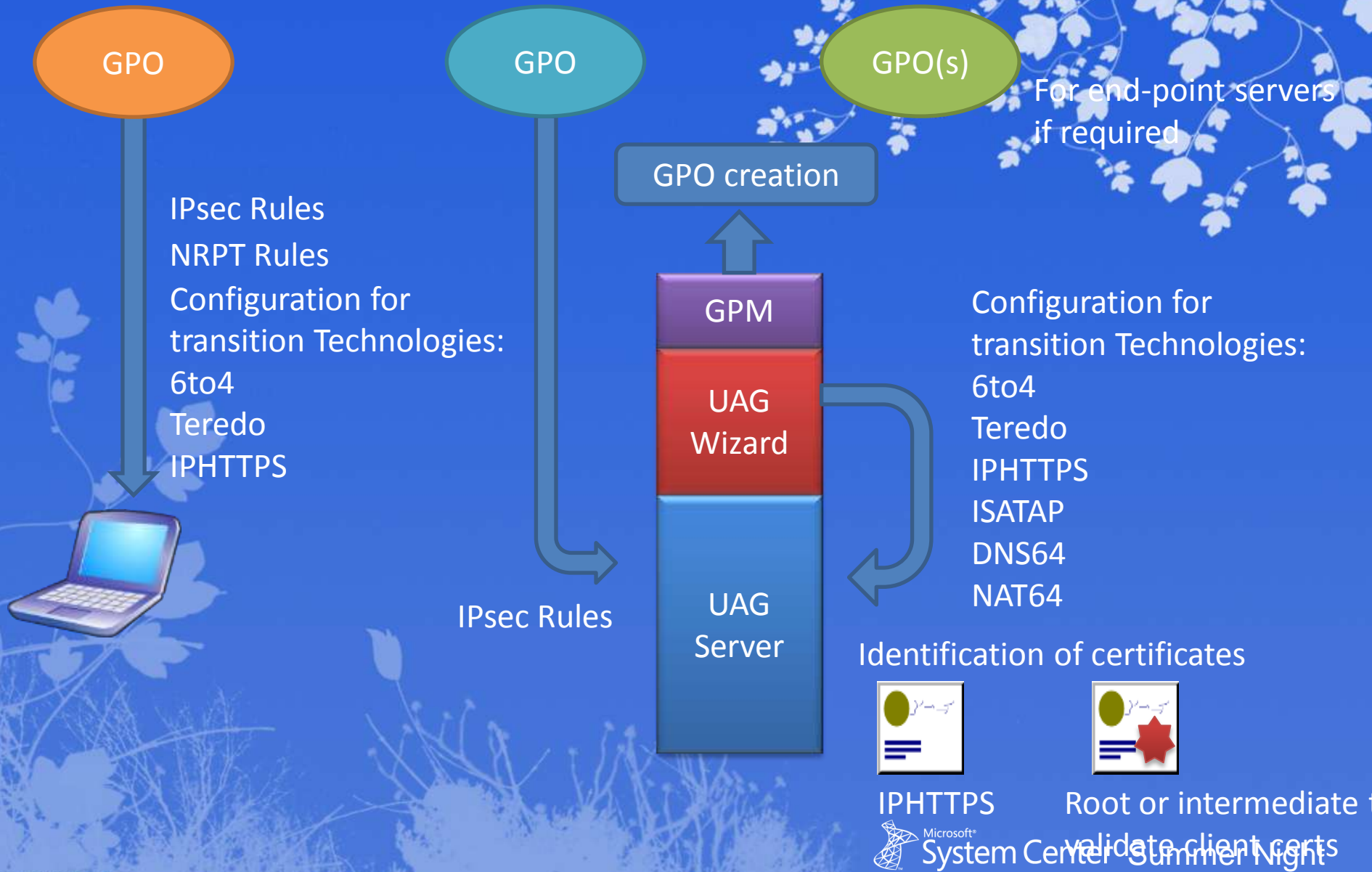
- End-to-end IPv6 & IPsec requires Windows Server 2008 or later
- Other models can use Windows Server 2003 or later

Infrastructure Technologies - Requirements

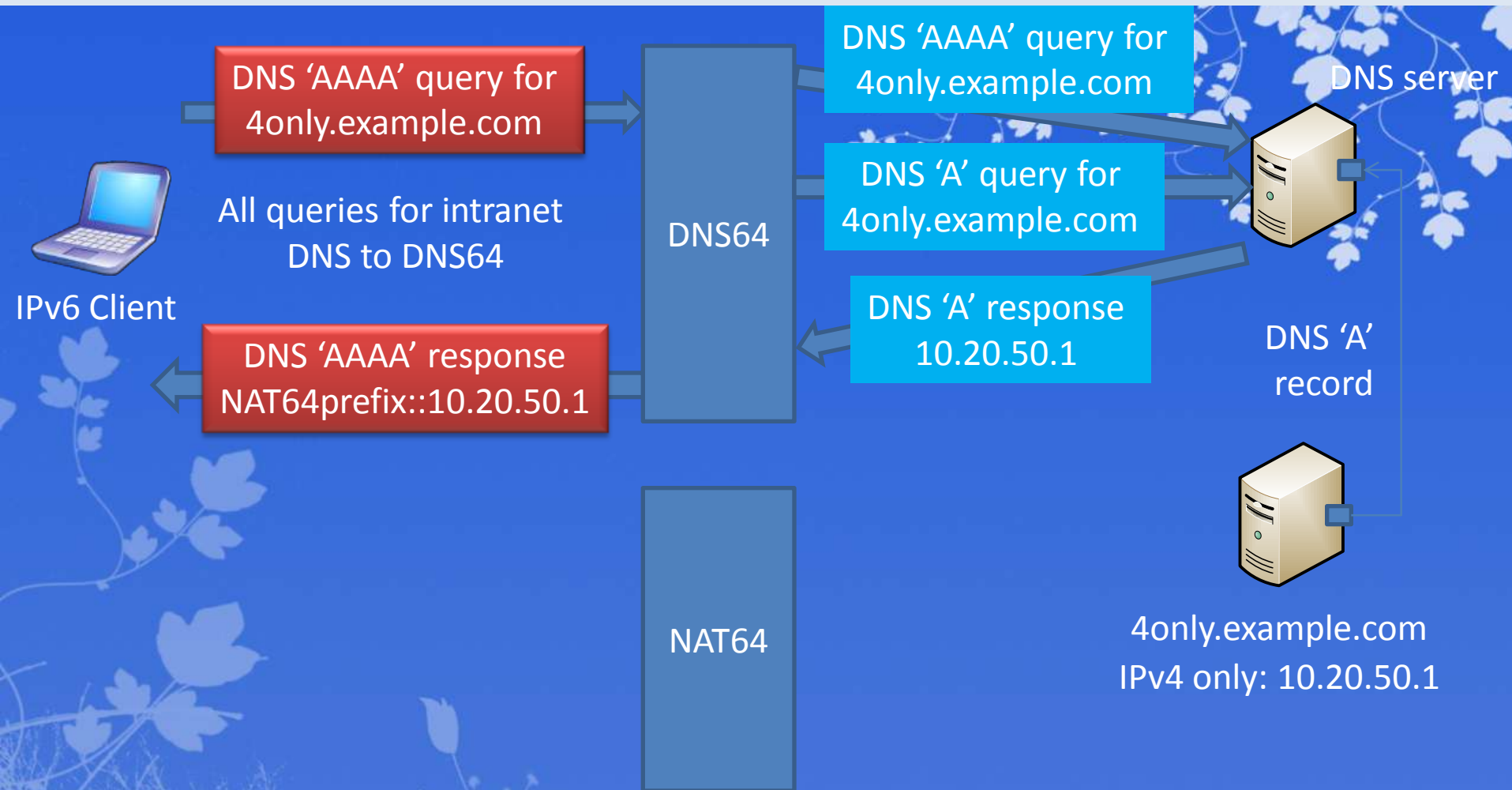
Don't configure DNS on the Internet facing adapters



DirectAccess Wizard



Infrastructure Technologies - DNS64



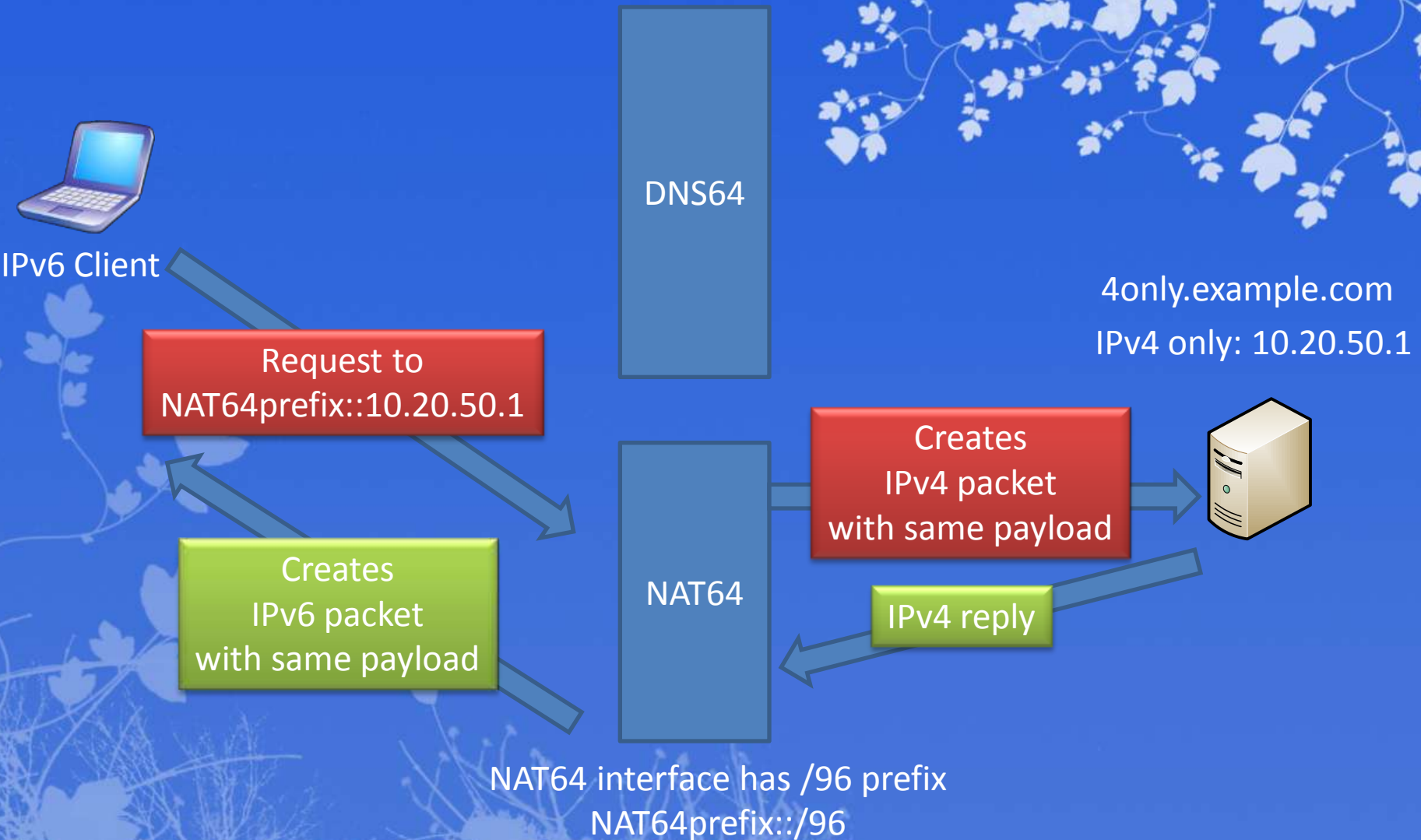
NAT64 interface has /96 prefix
NAT64prefix::/96



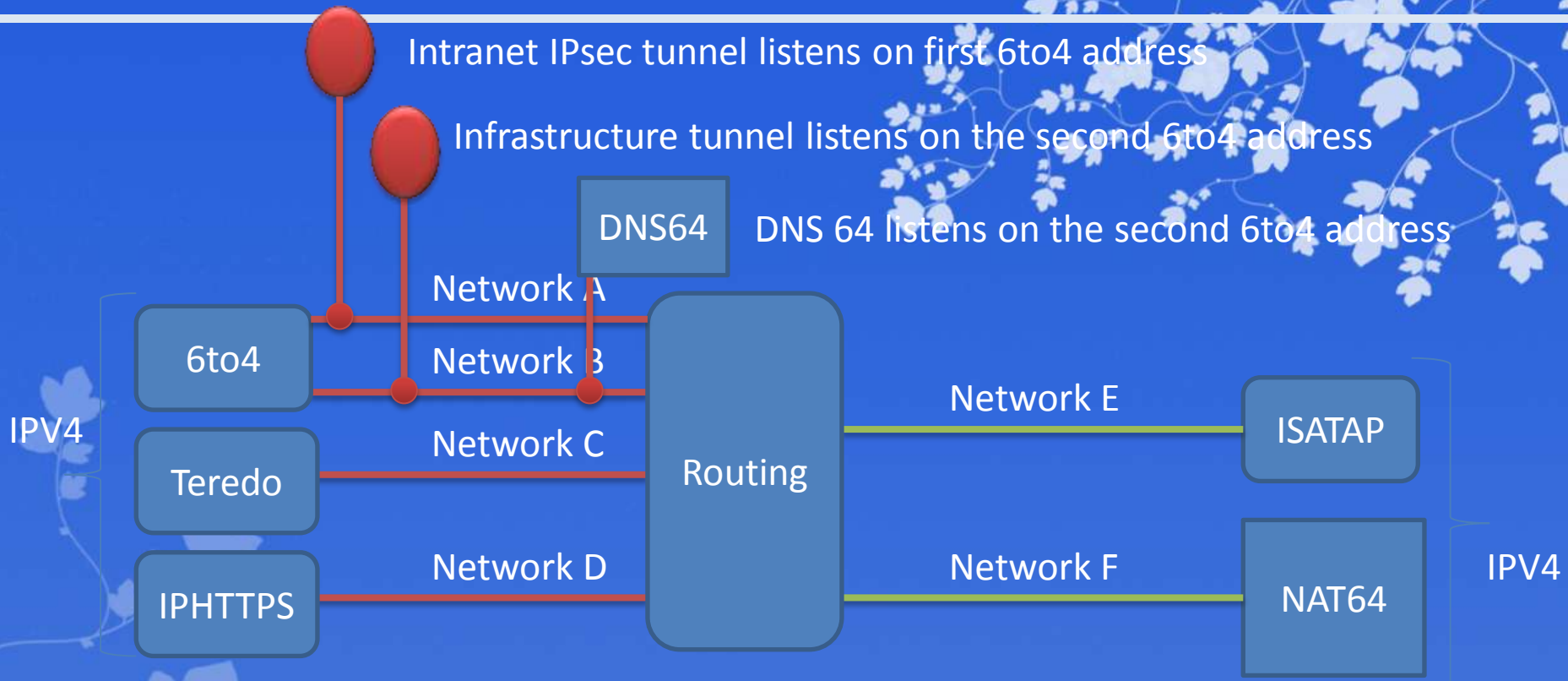
Microsoft

System Center Summer Night 29

Infrastructure Technologies - NAT64



Routing Traffic



- ❖ Traffic entering/leaving through the Internet facing tunnels must either be routed to/from the
 - ❖ ISATAP tunnel
 - ❖ NAT64 translator

Demo 2 – Security / Monitoring

Network Detection - Inside/Outside

- ❖ Used by DirectAccess Client to determine 'which' DNS Server to use based on namespace
- ❖ If the client can access an internal HTTPS website (https://nls.technocenter.nu)
 - Considered to be on the intranet
 - NRPT disabled
- ❖ No access to secure website
 - Considered to be on the Internet
 - NRPT remains enabled

Enter the name suffixes and IP addresses of internal DNS servers used to resolve DNS suffix queries.

	Name Suffix	IP address of DNS Server
▶	*.technocenter.nu	[DNS64]
	da.technocenter.nu	[Excluded]
	nls.technocenter.nu	[Excluded]
*	Double-click here to add...	

Network Detection - Inside/Outside

❖ DirectAccess client on the intranet

- ❖ Assumes not connected to intranet
- ❖ Establishes HTTPS connection to Network Location Server
- ❖ **RESULT: Domain WFAS Profile activated and NRPT disabled – No DA tunnels**

❖ DirectAccess client on the Internet

- ❖ Assumes not connected to intranet
- ❖ Fails to establish HTTPS connection to Network Location Server
- ❖ **RESULT: Public or Private Profile activated and NRPT enabled – DA tunnels activated**

Certificates

❖ UAG Server

- IP-HTTPS certificate
- Computer certificate

❖ DirectAccess Clients

- Computer certificate
- Health certificate if using NAP

❖ Network location server

- HTTPS certificate

❖ End-point servers using IPsec authentication/encryption

- Computer certificate

Monitoring

- ❖ Operations Manager 2007 R2
- ❖ Web Monitor
- ❖ PowerShell
- ❖ netsh - is your best friend ☺

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-DirectAccessUsers

ClientName
UserName
ArrayName
ClientID
Status
LastUpdated
LogonTime
HealthScore
TransitionTechnology
CertificateSubject

Administrator: C:\Windows\System32\cmd.exe
C:\Windows\system32> netsh interface teredo show state
Teredo Parameters
-----
Type           : client
Server Name    : 80.112.195.220 <Group Policy>
Client Refresh Interval : 30 seconds
Transit Server : unspecified
Client Port    : qualified
State          : teredo client
Client Type    : unmanaged
Network       : restricted
NAT            : UPMP: No, PortPreserving: Yes
NAT Special Behaviour : 10.0.0.190:61637
ArrayName     : External NAT Mapping : 193.173.108.5:61637
ClientName
UserName
ArrayName
ClientID
Status
LastUpdated
LogonTime
HealthScore
TransitionTechnology : Teredo
CertificateSubject :
```

The screenshot displays the Microsoft System Center Operations Manager 2007 R2 interface. The main window is titled 'Monitoring' and shows a 'DirectAccess NLB user activity' chart with a performance legend. The legend includes:

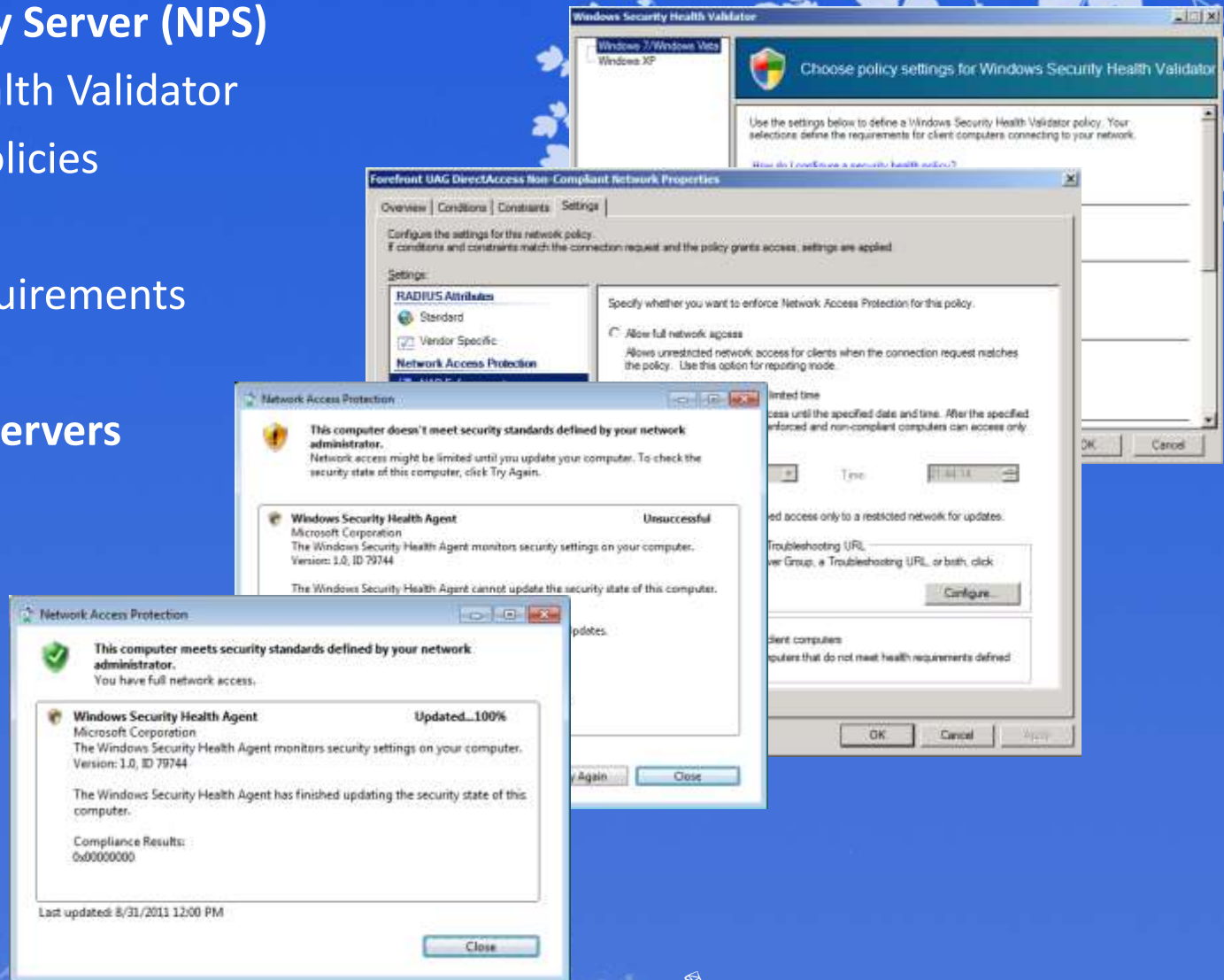
Show	Color	Path	Instance	Name
<input checked="" type="checkbox"/>	Blue	DAEDGE1.technocenter.nu	DirectAccess	Network load
<input checked="" type="checkbox"/>	Green	DAEDGE1.technocenter.nu	DirectAccess	User Kerberos
<input checked="" type="checkbox"/>	Red	DAEDGE2.technocenter.nu	DirectAccess	Network load balanced 6to4 and Teredo connect
<input checked="" type="checkbox"/>	Yellow	DAEDGE2.technocenter.nu	DirectAccess	User Kerberos Main Node SAs

On the right, the 'Event Viewer - All Events' window is open, showing a list of events:

Severity	Title	ID	Type	Category	Trust	NodeName	Description
Information	08/29/2011 16:20:18	84	Web Monitor Login	Security	FAK	DAEDGE1	The user TECHNOCENTER\admi...
Information	08/29/2011 16:20:18	84	Web Monitor Login	Security	FAK	DAEDGE2	The user TECHNOCENTER\admi...
Information	08/29/2011 16:20:02	84	Web Monitor Login	Security	FAK	DAEDGE1	The user TECHNOCENTER\admi...
Information	08/29/2011 16:20:02	84	Web Monitor Login	Security	FAK	DAEDGE2	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:52	84	Web Monitor Login	Security	FAK	DAEDGE1	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:52	84	Web Monitor Login	Security	FAK	DAEDGE2	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:47	84	Web Monitor Login	Security	FAK	DAEDGE1	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:47	84	Web Monitor Login	Security	FAK	DAEDGE2	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:42	84	Web Monitor Login	Security	FAK	DAEDGE1	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:42	84	Web Monitor Login	Security	FAK	DAEDGE2	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:41	84	Web Monitor Login	Security	FAK	DAEDGE1	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:41	84	Web Monitor Login	Security	FAK	DAEDGE2	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:27	84	Web Monitor Login	Security	FAK	DAEDGE1	The user TECHNOCENTER\admi...
Information	08/29/2011 16:19:27	84	Web Monitor Login	Security	FAK	DAEDGE2	The user TECHNOCENTER\admi...

Network Access Protection (NAP)

- ❖ Network Policy Server (NPS)
 - ❖ System Health Validator
 - ❖ Network Policies
- ❖ HRA Server
 - ❖ Health Requirements
- ❖ NAP CA
- ❖ Remediation Servers
 - ❖ WSUS
 - ❖ SCCM



Summary

- ❖ **More Productive**
- ❖ **More Secure**
- ❖ **More Manageable and cost effective**
- ❖ **Starting point IPv6 Readiness**
- ❖ **Cloud Readiness**
 - Publishing Private Cloud
 - Key components still remain on-premise
 - Office 365 federations with Active Directory

Questions & Answers

Resources

❖ **DirectAccess Home Page**

<http://technet.microsoft.com/en-us/network/dd420463.aspx>

❖ **Test Lab Guides (TLG)**

<http://technet.microsoft.com/en-us/library/gg617324.aspx>

❖ **IPv6 Survival Guide**

<http://social.technet.microsoft.com/wiki/contents/articles/ipv6-survival-guide.aspx>

❖ **SCUG BLOG**

<http://scug.nl>

❖ **Inovativ BLOG**

<http://blogs.inovativ.nl>

Microsoft®
System Center
User Group **Nederland**

inovativ 
..de System Center specialisten

 Microsoft®
System Center Summer Night