

DirectAccess

簡志偉 Kevin Chien

大型企業業務暨經銷事業群

台灣微軟

議程大綱

- 安全的存取
- Demo
- DirectAccess 解決方案
 - 效益
 - 部署需求
- 名稱解析
- 支援的技術

行動工作



範圍越來越
擴大

行動資料

全球化



“重新定義範圍”

“我的網路就是我的建築物所在的位置”



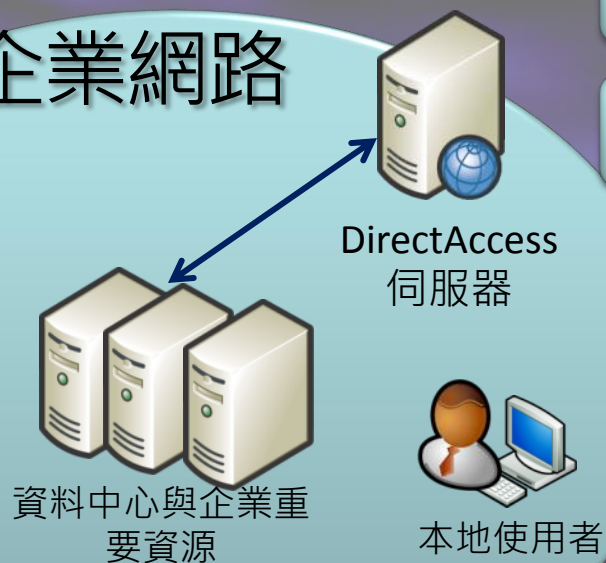
- 如何隨時管理、監控與支援遠端使用者/機器?
- 如何簡化遠端工作者的存取



“我的網路就是我的使用者與資產的位置”

產業趨勢

企業網路



假設基本的網路總是不安全

重新定義企業邊界來保護資料中心

以身分為基礎的安全原則，而非地點

網際網路



Windows Server 2008 R2

解決客戶的需求



解決使用者需求



支援 IT 專業人員

使用 Direct Access 建立在任何地方都能工作的架構

DirectAccess

- 提供無縫式與安全地從任何地方存取企業資源



DEMO

DirectAccess

Direct Access 的效益

將企業網路帶給使用者

更具生產力

- 漫遊時可持續與企業網路保持連結
- 不需使用者動作就可以工作
- 不管在公司內部還是在公司外的使用體驗皆相同



更安全

- 健康的與可信賴的主機
- 每一程式/伺服器原則管控
- 在資產周邊更豐富的原則管控
- 有能力延伸法規遵從到漫遊資產
- 增加部屬的路徑到 IPv6



更好管理與成本效益

- 簡化的行動資源的遠端管理，就如同它們都在內部網路一樣
- 較低的TCO以及“總是被管理的”基礎架構
- 跨越所有情境與網路的整合的安全存取
- 所有連線機制的整合管理



Always On

- 順暢地連線
- 不需使用者動作
- 適應不斷變化的網路

安全

- 預設加密
- 可結合智慧卡
- 多種存取管控
- 與現有的各項原則
共存





容易管理

- 接觸到之前碰不到的機器
- 允許遠端用戶端可以套用群組原則
- 整合 NAP 進行健康狀態檢查
- 聯合周圍的基礎架構

VPN vs. DirectAccess – 價值比較



Internet

DirectAccess 用戶端
(Windows 7)

DirectAccess 伺服器
(Server 2008 R2)

建立在 IPv4 UDP, HTTPS
等等的通道

加密的 IPsec+ESP

加密的 IPsec+ESP

原生 IPv6

6to4

Teredo

IP-HTTPS

IPsec Gateway

在企業內啟動 IPv6

選項 1 - ISATAP

DirectAccess Server
(Server 2008 R2)

Line of Business
Applications



IPv4



Windows Server 2008/R2

- Client for Microsoft Networks
- QoS Packet Scheduler
- File and Printer Sharing for Microsoft Networks
- Internet Protocol Version 6 (TCP/IPv6)
- Internet Protocol Version 4 (TCP/IPv4)
- Link-Layer Topology Discovery Mapper I/O Driver
- Link-Layer Topology Discovery Responder

在企業內啟動 IPv6

選項 2 – NAT-PT

DirectAccess Server
(Server 2008 R2)

Line of Business
Applications

Windows Server 2003
Non-Windows

NAT-PT
DNS-ALG

IPv6

IPv4

- Client for Microsoft Networks
- QoS Packet Scheduler
- File and Printer Sharing for Microsoft Networks
- Internet Protocol Version 6 (TCP/IPv6)
- Internet Protocol Version 4 (TCP/IPv4)
- Link-Layer Topology Discovery Mapper I/O Driver
- Link-Layer Topology Discovery Responder

企業網路

DirectAccess Server
(Server 2008 R2)

Line of Business
Applications



No IPsec

只有 IPsec 完整性
性 (認證)

IPsec 完整性+
加密

Windows Server 2003
Windows Server 2008
Non-Windows Server

IPsec Gateway



IPsec Hardware Offload Supported

DirectAccess 使用者介面

DirectAccess 已
可使用!

內建除錯功能

Currently connected to:

- Interwebs**
Corporate and Internet access
Wi-Fi

Available networks:

- Clearwire
Wi-Max
- Verizon
Wi-Fi
- Flyingbit
Wi-Fi
- Myweb
Wi-Fi

Open Network and Sharing Center

Turn off notification of new networks

Diagnose and repair

Network and Sharing Center



Fix a network problem

Diagnose and repair network problems, or get troubleshooting information.



部署需求

部署需求



DirectAccess 用戶端

- 需要 Windows 7 企業版或旗艦版
 - 須加入網域
- 連線到公司網路的起始流程



DirectAccess 伺服器

- 需要 Windows Server 2008 R2
- 位於公司網路邊界



應用程式伺服器

- 端對端的 V6 & IPsec 需要 Windows Server 2008 或以上
- 其他模組可使用 Windows Server 2003 或以上

部署需求



DC/DNS

- 需要至少一台 W2K8 SP2 或 R2 DC/DNS 伺服器提供 V6 紀錄在用戶端的註冊



網路架構

- 可以是 IPv4 因為我們使用 ISATAP with DirectAccess



NAT-PT

- 可以被使用來提供存取到 IPv4-only 的資源

名稱解析

Name Resolution Policy Table

(名稱解析原則表)

- 在 Windows 7 的新功能
- 被使用在 DirectAccess 用戶端上，根據名稱解析來決定使用 '哪一個' DNS 伺服器
- 新的名稱解析順序：
 - 本機快取
 - 主機檔案
 - 名稱解析員則表 (NRPT)
 - DNS

支援的技術

Direct Access 支援的技術

可信賴的, 安全的,
健康的機器



Windows 7 用戶端



NAP (包含伺服器與網域隔離 [SDI])



Forefront Client Security



Windows 防火牆



BitLocker + 可信賴平台模組 (TPM)



IAG SP2



Forefront UAG



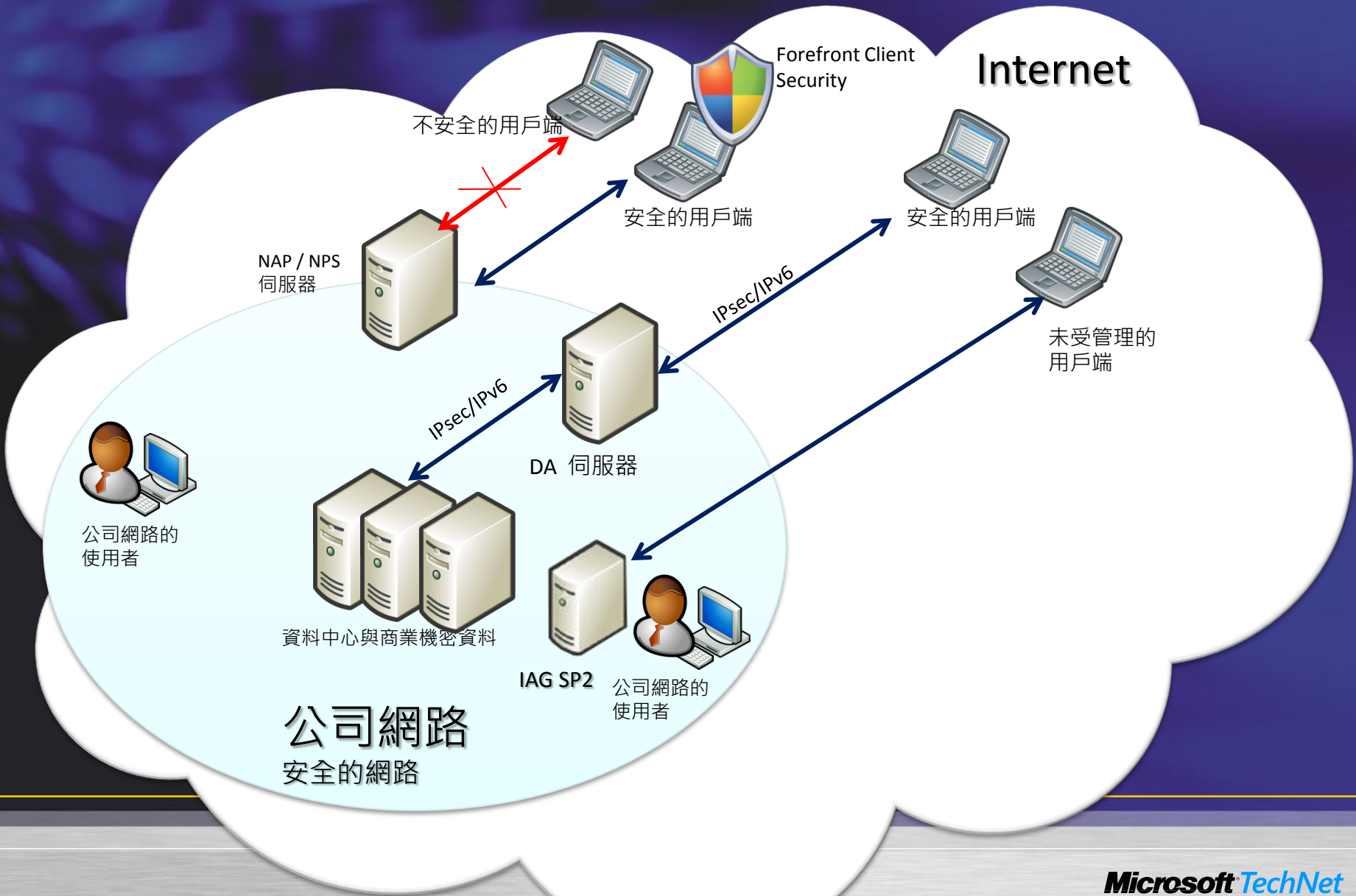
企業網路

DC & DNS
(Server 2008 R2)



應用程式 & 資料

Direct Access 支援的技術



總結

- Windows Server 2008 R2 提供更好的創新讓
您隨時隨地都可以進行存取
- 多了解 Direct Access
- 開始著手部署 Windows Server 2008
- <http://www.microsoft.com/directaccess>

Microsoft[®]

Your potential. Our passion.[™]

© 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.