DirectAccess:
Anywhere Access for Windows

William Dixon
Principal Consultant/Architect
Microsoft Consulting Services

DirectAccess
Server and Domain Isolation - protecting internal systems & traffic with IPsec
Network Access Protection (NAP) – end point health assessment, enforcement
General Windows security -Active Directory, smartcards, PKI, hardening, DNSSec
Today’s Agenda

1. Introduction to DirectAccess
2. Technical Introduction
3. Technical Details within Demo
4. Summary
Section 1:
Introduction to DirectAccess
Increasingly Porous Perimeter

Mobile Workforce

Mobile Data

Globalization
Network Access Vision

Enterprise Network

Datacenter Servers

Local Client

Remote Client

Internet

**Identity:** Strong authentication required for all users

**Authorization:** Computer health is validated or remediated before allowing network access

**Protection:** All network transactions are authenticated and encrypted

Policies are based on identity, not on location
DirectAccess

Extending network services and resources to remote users
# DirectAccess: More than Remote Access

<table>
<thead>
<tr>
<th>Always On</th>
<th>Manage Out</th>
<th>Access Policies</th>
<th>Protected Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved productivity</td>
<td>&quot;Light up&quot; remote clients</td>
<td>Pre-logon health checks and remediation</td>
<td>Supports authenticated transactions</td>
</tr>
<tr>
<td>Not user initiated</td>
<td>Decreases patch miss rates</td>
<td>Replaces modal &quot;connect-time&quot; health checks</td>
<td>Supports encrypted transactions</td>
</tr>
<tr>
<td>Simplified connectivity</td>
<td>Applies GPOs to remote computers</td>
<td>Full NAP integration</td>
<td>Authentication and encryption mitigate many attacks</td>
</tr>
</tbody>
</table>

VPN: connect

DirectAccess: extends
Section 2:
Technical Introduction
Data Center and Business Critical Resources

NAP/NPS Health Servers

DirectAccess Thin Edge, Low Cost

Compliant Client

Internet

Clients have transparent IPv6 corpnet connectivity from anywhere with IPsec security

Traffic to corporate network is routed through a Direct Access Server (Windows 2008 R2 Server role)

Integrates with NAP IPsec enforcement for policy-based perimeter (optional)

IPv6 tunnel over IPv4
Then IPv6 IPsec tunnel inside

CORPNET Compliant Network
Forefront UAG and DirectAccess: Better Together

- Supports many non-DA clients
- Enables DA client access to IPv4-only internal hosts with DNS64/NAT64
- Enhances DA scalability and management
  - High avail, load balancing
  - Monitoring, Reports
- Provides OTP user auth
- Simplifies deployment and administration
  - Easy Setup Wizard
  - Auto GPO, script gen
  - DA Connectivity Assistant
- Delivers a hardened, edge-ready solution using Forefront Threat Management Gateway firewall core
Remote Client Management Only

- Only the first IPsec infrastructure tunnel is established. Clients have access only to specific infrastructure servers.
- Remote management includes:
  - Active Directory Group Policy, login scripts
  - Pull or push* software updates, AV updates – using same internal mgmt servers
  - Client health checking, reporting and remediation
  - Client monitoring, vulnerability scanning; software inventories
  - Help desk connect out* via Remote Assistance, Remote Desktop

* Internally initiated connections outbound to remote DA client requires IPv6 path (e.g. internal native IPv6 or ISATAP), and dynamic DNS update by client

IPv6 Address

[Diagram showing network infrastructure and connections]
Selective Access to Full Intranet Access

- Provides client remote management and allows computer and user access to internal resources
  - Infrastructure tunnel for computers
  - Selected servers, prefixes, or full Intranet access
- Different authentication requirements possible:
  - Computer/user domain password (not IKE Preshared Key)
  - Computer/user certificate
  - Computer/user Kerberos
  - User smartcard, OTP (with UAG)

IPv6 Address

Intranet Tunnel
DirectAccess Supporting Technologies

Trusted, authorized machine + compliant (NAP)

- Domain Password
- Certificate
- Trusted, Authorized user
- Domain Password
- Certificate
- Smartcard
- One Time Password (with UAG)

Windows 7 client

Windows Firewall
- Group Policy: Inside/Outside URL DNS settings IPsec policy Certificate settings
- BitLocker + Trusted Platform Module (TPM)

Corporate Network
- Applications & Data
- DC & DNS
- PKI
  - Provides Computer certificate
- Windows System Health Agent (SHA)
  - checks Windows Security Center Status
  - Custom SHAs available from many 3rd parties

NAP Health Certificate
- AntiMalware AntiSpyware
- Firewall
- Update Status e.g. Windows Update, WSUS, SCCM/SMS Agent
The Forefront Business Ready Security hosted VM demo environment supports a DirectAccess server, a DirectAccess client and an ISATAP enabled internal network.

Choose lab duration 1-4 hours, can save/pause
Takes about 2-5 minutes to start up
Click on host name to get an automatic RDP workspace

Uses IPv4 public range addresses for Internet inside virtual "Internet" network only. These do not correspond to real Internet address uses. Addressing may change in future versions of the lab.
Section 2: Technical Details
DirectAccess:
Technical Foundation

Name Resolution:
DNS and NRPT

Data Protection:
IPsec

Connectivity:
IPv6
DirectAccess & Enabling IPv6

DirectAccess Client

- Native IPv6
- 6to4
- Teredo
- IP-HTTPS

Internet

DirectAccess Server

- Transition Mechanism Tunnels over IPv4
Internal IPv6 Connectivity:

**Native IPv6**
- Works with any server OS that supports IPv6
- Requires IPv6 network infrastructure
- Delivers best choice over time

**ISATAP**
- Tunnels IPv6 inside IPv4
- Doesn’t require routing infrastructure upgrades
- Requires Windows Server 2008 or R2

**DNS64/NAT64**
- Translates IPv6 to IPv4
- Works with any server OS
- Is available in Forefront UAG

---

**IPv6 Options**

DirectAccess works best if the corporate network has native IPv6 deployed.

**Internet**

**Intranet**

- Native IPv6
- IPv6 Transition Technologies
- IPv4

---

[Diagram showing network connectivity and options for IPv6 deployment]
External IPv6 IPsec

Internet

DirectAccess
Client

6to4, Teredo, IP-HTTPS
IPv6 encrypted IPsec ESP tunnel

IPv6 encrypted IPsec ESP tunnel

IPv6 IPsec Gateway

Native IPv6 IPsec Hardware Offload Supported
DirectAccess traffic is protected by two IPsec tunnels
- Infrastructure tunnel relies on computer authN only
- Intranet tunnel relies on computer + user authentication

Identify which resources will be available in first tunnel
- DCs/DNS, SCCM, AV servers – anything machines need to connect w/o user being logged on
- Computer authN only elevates the risk – be selective!
IPv6 IPsec Tunnel Detail

- AuthIP protocol used to negotiate IPsec tunnels
- AuthIP tracks host security context that sends packet: computer or user
- Two independent authentications for each tunnel
- 1st Auth - Main Mode – Always computer authentication
- 2nd Auth – Extended Mode – computer or user auth, depending on packet
- Supports computer/user password auth, certificates, Kerberos, smartcards – no PSK
- IPv6 IPsec tunnel destination addresses are 6to4 addresses derived from public IPv4 IPs using within the lab (these addresses are only used within the virtual lab, not Internet)
IPv6 IPsec Infra Servers Tunnel

- **List of Dest Infra Servers:**
  - IPv6 Addresses (DC, DNS, etc)

- **IPv6 IPsec Intranet Tunnel Rule:**
  - NAT64 /64 Prefix for Traffic Inside Intranet Tunnel
  - DA Server 6to4 Tunnel Addresses

- **Different Authentication Options Available for Infrastructure Server Tunnel vs. Rest of Intranet Tunnel:**
  - 1st Authentication Methods
    - Computer Certificate
    - None
  - 2nd Authentication Methods
    - User (NTLMv2)
    - User (Kerberos V5)
Additional End-to-End IPsec Authentication

IPv6 Address

DA Clients (Win7)

IPv6 IPsec tunnel (inside IPv6overIPv4 tunnel)

IPv6 IPsec transport mode security associations provide end-2-end through IPv6 IPsec tunnel

- If IPv6 available on internal network, IPsec transport mode possible
- IPsec transport can encrypt or just authenticate
- Provides fine-grained policy-based control on internal ho
**Name Resolution Policy Table (NRPT)**

- Group Policy NRPT settings require DirectAccess clients to use internal DNS servers for internal namespaces
  - Clients can be required to use specific DNS servers for different DNS namespaces
  - Optionally, DNS queries for specific namespaces can be secured using IPSec
  - Single-label names (e.g. http://sharepoint) first get DNS suffix append

<table>
<thead>
<tr>
<th>Namespace</th>
<th>DNS Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.woodgrovebank.com</td>
<td>2002:2701:104::2701:104 (UAG DNS64)</td>
</tr>
<tr>
<td></td>
<td>2001:DB8:1234::1234 (internal IPv6 DNS if avail)</td>
</tr>
<tr>
<td>nls.woodgrovebank.com</td>
<td>None, exemption (network location server)</td>
</tr>
<tr>
<td>*.extranet.woodgrovebank.com</td>
<td>None, exemption if extranet namespace is within internal namespace so that clients can use public DNS servers IPs instead of redirecting</td>
</tr>
</tbody>
</table>

Netsh name show policy – the configured NRPT settings, may or may not be active

Netsh name show effective – the currently active NRPT settings
DNS64

DA Client resolve name of an IPv4 only server to IPv6 address

<table>
<thead>
<tr>
<th>Namespace</th>
<th>DNS Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.woodgrovebank.com</td>
<td>2002:2701:104::2701:104 (UAG DNS64)</td>
</tr>
<tr>
<td>nls.woodgrovebank.com</td>
<td>None, exemption (network location server)</td>
</tr>
<tr>
<td>*.extranet.woodgrovebank.com</td>
<td>None, exemption if extranet namespace is within internal namespace so that clients can use public DNS servers IPs instead of redirecting</td>
</tr>
</tbody>
</table>
NAT64

DA Client sends an IPv6 packet to the IPv6 NAT64 destination address to reach IPv4 host

Send packet to:
2002:2701:104:8000::A01:203

Packet to: 10.1.2.3

Host name: x.woodgrovebank.com
IP: 10.1.2.3

DNS64/NAT64 Tradeoffs:
- Obviates the need for IPv6 on intranet or internal hosts
- Does not enable outbound connect to DA client
- Does not allow IPv6 IPsec end-to-end
- Makes IPsec tunnel rules more difficult with NAT64 addresses

UAG uses NAT64 Prefix: 2002:2701:104:8000::/96
Network Location Determination

- Group Policy configures:
  - A “domain location determination server” FQDN, also called a network location server (NLS)
  - Name Resolution Policy Table (NRPT), which must exempt this NLS server name

- Client connects to network, assumes it is “outside”:
  - “Public” profile of Windows Firewall used, with DirectAccess IPsec rules
  - NRPT active, does not redirect DNS resolution for NLS

- Attempt https to NLS, if reachable, then “inside”:
  - “Domain” profile of Windows Firewall used, no DirectAccess IPsec rules
  - NRPT not active
Supports Split Tunneling or Forced Tunneling

- DirectAccess implements split-tunneling by default
- Can enable Force Tunneling option
  - Uses IP-HTTPS only
  - Once established, no IPv4 connectivity except local subnet, must either route or use internal proxy to Internet
Multi Factor Credentials for Intranet Access

Two Factor Authentication (TFA) is fully supported, but not required

Edge-based enforcement is a smarter way to enforce TFA

Users are assigned a well-known SID when they log on with a smartcard (S-1-5-65)

Users may log on to a laptop without TFA

When users access corporate resources, the IPsec tunnel authorization policy checks for the SID

Provide your OTP credentials for full corporate access

Windows needs your smart card credentials. Windows needs your smart card credentials to access your corporate network. Click to enter your credentials or lock this computer, and then unlock it using your smart card.
NAP Health for Clients (Optional)

- NAP Health Certificate says client is “healthy” or “compliant” to policy
- NAP Health Registration Authority (HRA) – receives client cert request
- NAP Network Policy Server (NPS) - validates health claims, decides whether compliant or not to policy settings
- Supports reporting-only mode, deferred enforcement, full enforcement
- Enforce health on Intranet Tunnel unless HRA and remediation on Internet
Deployment Resources

- Windows IPv6 Book, IPv6 Hands On Labs
  http://microsoft.com/ipv6

- Forefront Online Virtual Labs (have IPv6 enabled)
  http://technet.microsoft.com/hi-in/virtuallabs/bb499665
  http://www.mssalesdemos.com – Business Ready Security

- Forefront UAG 2010 SP1 Eval Download:

- Forefront UAG SP1 Lab Guides
  http://technet.microsoft.com/hi-in/virtuallabs/bb499665

- Detailed Windows and UAG Design Guides
  http://www.microsoft.com/directaccess
  http://www.microsoft.com/uag

- Microsoft Consulting Service DirectAccess solution
- Microsoft Partners
- UAG Appliance Vendors
## DirectAccess:
More than Remote Access

<table>
<thead>
<tr>
<th>Always On</th>
<th>Manage Out</th>
<th>Access Policies</th>
<th>Protected Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improved productivity</td>
<td>&quot;Light up&quot; remote clients</td>
<td>Pre-logon health checks and remediation</td>
<td>Supports authenticated transactions</td>
</tr>
<tr>
<td>Not user initiated</td>
<td>Decreases patch miss rates</td>
<td>Replaces modal &quot;connect-time&quot; health checks</td>
<td>Supports encrypted transactions</td>
</tr>
<tr>
<td>Simplified connectivity</td>
<td>Applies GPOs to remote computers</td>
<td>Full NAP integration</td>
<td>Authentication and encryption mitigate many attacks</td>
</tr>
</tbody>
</table>

VPN connect the user to the network
DirectAccess extends the network to the computer and user
Requirements for DirectAccess

Customer Knowledge
- Should have a basic working knowledge of IPsec or TCP/IP
- Should be interested in learning and deploying new technologies, such as IPv6

DirectAccess Clients
- Windows 7 Enterprise Edition or Windows 7 Ultimate Edition
- Server 2008 R2 Standard Edition or Higher
- Domain-joined computers

DirectAccess Server
- Windows Server 2008 R2, Standard Edition or Higher
- Domain-joined computers

Others
- DNS Servers Supporting DirectAccess Clients - Windows Server 2008 SP2 or later for IPv6 internally
- A public key infrastructure (PKI) to issue computer certificates, smart card certificates, and, for NAP, health certificates.
Addendum: DirectAccess vs. VPNs

Benefits of DirectAccess Over Traditional VPNs:
- Connects the client computer automatically, without initiation by the user
- Works through all firewalls
- Supports selected server access and IPsec authentication with an Internet network server
- Supports end-to-end authentication and encryption
- Supports management of remote client computers

VPNs Still Provide Remote Access for:
- Windows Vista® and earlier versions of Windows client computers
- Client computers running non-Microsoft operating systems
- Non-domain joined computers