Helsinki Metropolia University of Applied Sciences
Degree Programme in Information Technology

Jani Myllyviita

DirectAccess Implementation for Corporate Infrastructure

Bachelor's Thesis. 19 April 2010

Supervisor: Markku Nuutinen, Principal Lecturer
Language Advisor: Marianne Kiekara, Lecturer

Helsinki Metropolia University of Applied Sciences **Abstract**

Author Title Number of Pages Date	Jani Myllyviita DirectAccess implementation for corporate infrastructure 22 19 April 2010
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Supervisor	Markku Nuutinen, Principal Lecturer

The goal of this study was to find out how the remote access software Microsoft Forefront Unified Access Gateway operates and how it can be efficiently managed. The study focuses on the DirectAccess feature, which allows automatic connection to a corporate network that utilizes a Windows server domain. It also describes how the Forefront Threat Management Gateway is connected to UAG.

A virtual test lab environment was used to perform most tests and the implementation described in the study was also deployed in a production environment.

This study does not include the deployment of the underlying Active Directory services. It also assumes that the network has a Windows Server 2008 R2, which is necessary for the DirectAccess feature. The client computers must run Windows 7 operating system to be able to take advantage of the DA feature.

The results showed that with a moderate amount of configuration it is possible to deploy a remote access server for end users and that the configuration can be easily spread to client computers.

Keywords	DirectAccess, UAG, remote access

Metropolia Ammattikorkeakoulu **Insinöörityön tiivistelmä**

Tekijä Otsikko Sivumäärä Aika	Jani Myllyviita DirectAccess-toteutus yrityksen infrastruktuurissa 22 19.4.2010
Koulutusohjelma	tietotekniikka
Tutkinto	insinööri (AMK)
Ohjaava opettaja	yliopettaja Markku Nuutinen

Tämän insinöörityön tavoitteena oli selvittää, miten etäkäyttöohjelma Microsoft Forefront Unified Access Gateway toimii ja miten sitä voidaan hallita tehokkaasti. Tutkimus keskittyy DirectAccess-ominaisuuteen, joka mahdollistaa automaattisen yhteyden yrityksen Windows-toimialueverkkoon. Työssä kuvataan myös, miten Forefront Threat Management Gateway on kytketty UAG:hen.

Useimmissa testeissä käytettiin virtuaalista testiympäristöä, ja vastaavaa toteutusta on käytetty myös tuotantoympäristöissä.

Työstä rajattiin pois toimialuealustan käyttöönotto. Työssä oletetaan, että yrityksellä on valmis infrastruktuuri, josta löytyy Windows Server 2008 R2 -palvelin, joka on yksi DirectAccess-ominaisuuden edellytys. Lisäksi työasemissa täytyy olla Windows 7 -käyttöjärjestelmä.

Tulokset osoittivat, että kohtuullisen määrittelyn jälkeen on mahdollista ottaa käyttöön etäkäyttöpalvelin ja tarvittavat asetukset on helppo jakaa työasemille.

Hakusanat	DirectAccess, UAG, etäkäyttö

Contents

Abbreviations

CA	Certificate Authority
DA	DirectAccess
DC	Domain Controller
DMZ	Demilitarized Zone (Perimeter Network)
DNS	Domain Name System
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
GPO	Group Policy Object
IAG	Intelligent Application Gateway
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISA	Microsoft Internet Security and Acceleration Server
ISAKMP	Internet Security Association and Key Management Protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
LAN	Local Area Network
NAP	Network Access Protection
NAT	Network Address Translation
NAT-PT	Network Address Translation/Protocol Translation
NLS	Network Location Server
NRPT	Name Resolution Policy Table
NTLM	NT LAN Manager
PKI	Public Key Infrastructure
TMG	Microsoft Forefront Threat Management Gateway
UAG	Microsoft Forefront Unified Access Gateway
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network (commonly the Internet)

1 Introduction

This study describes the necessary components for a DirectAccess implementation in an existing Windows Active Directory infrastructure. The system has been deployed in a few different environments including some test labs that were completely virtual.

The key feature of DirectAccess is mobility, which helps end users be more productive. Employees need access to their corporate resources when working remotely or while on customer premises. For a long time they have had to use inconvenient software to open secure VPN tunnels to their company networks or use web- based portals to open their network resources.

Microsoft introduced DirectAccess in Windows Server 2008 R2 and Windows 7. This feature provides automatic connectivity to the corporate LAN without user interaction. The basic concept is to establish a secure tunnel over the Internet by authenticating with the computer certificate that has been issued by the corporate Certificate Authority and can be verified by the UAG server.

This study describes the basic components necessary for a simple DirectAccess implementation. The first two chapters cover the server requirements and UAG installation with DirectAccess configuration. The next chapter details how some UAG components work in more detail. The next chapters deal with the necessary changes and additions to the existing infrastructure to handle the client connections. These changes include DNS and AD additions and modifications in addition to certificates.

Microsoft has extensive documentation on DirectAccess and the UAG in their TechNet library [1]. Also the TechNet blogs have several very good entries discussing the common problems and technical implementations that are used for DirectAccess among other topics [2]. Many of these articles and blogs have helped understand the mechanics of UAG.

The main benefit of deploying DirectAccess is the ease of access for end users to the corporate resources. The ability to use basically any Internet capable connection to automatically establish the tunnel makes the end user experience much simpler. This study does not focus on the underlying infrastructure. It is assumed that the corporation already has a working Active Directory implementation with Windows Server 2008 R2, Windows 7 workstations and a Certificate

Authority role on one server. This implementation uses the ISATAP IPv6 transition technology to allow DirectAccess client connections to the current IPv4 LAN infrastructure.

The main goal of this study was to find out how DirectAccess is implemented and how all the necessary components of the system work. In other words: How does it all come together and how all configurations are managed? From an administrator's perspective the initial configuration should be complete so that it does not have to be modified unless some bigger changes are necessary.

2 Unified Access Gateway

UAG is part of the Microsoft Forefront security line of products [3]. The previous version was known as Intelligent Application Gateway. IAG was Microsoft's VPN solution before DirectAccess. It also provided a web portal for published applications similar to the new UAG. In this study the web portal feature of UAG is not covered.

2.1 UAG Installation

The server for UAG can be a modern dual-core physical or a virtual 64-bit server. It is recommendable to have at least 4 GB of memory for the machine [4]. UAG needs at least two network adapters. One connected to the DMZ/WAN and another to the LAN. The server has to be running Windows Server 2008 R2 Standard or Enterprise. A DirectAccess server must be a member of an Active Directory domain. If only a single server is deployed, it is still a good idea to put it into an array for future scalability. During the UAG installation TMG will also be installed on the server as a prerequisite.

DirectAccess requires two consecutive public IP addresses for normal operation. The consecutive IP addresses are used by UAG to act as a Teredo server. Depending on the implementation it also needs a local IPv4 or an IPv6 address. In this study the focus is on an IPv4 implementation with ISATAP. In lab tests the public IP address requirement was noticed after getting an unusual error message stating the 6to4 network interface could not be enabled. After some troubleshooting it was discovered that the lab-assigned public range was actually within the private 10.0.0.0/8 range. [5]

The UAG can be connected straight to the Internet or through a corporate firewall but it cannot be behind a NAT. The internal TMG firewall can secure the server but the corporate security policies may dictate that the connection must go through a dedicated firewall.

2.2 UAG Configuration

The basic configuration consists of three steps and is guided by the configuration wizard. First the network configuration must be defined so UAG knows which network is behind each network

adapter. Every network adapter must be linked to either the internal network, external network or be left as unassigned. The configuration also needs to know the internal IP address ranges for the TMG network object.

The second part is the UAG topology configuration. A server can be in an array or it can be run as a standalone. For scalability it is usually preferred to make an array so additional servers can later be added if necessary. A server can also be joined into an array after the initial configuration. The array storage is located on a domain controller so UAG needs an Active Directory service account to access the files.

The third setting defines whether updates are desired from Microsoft for UAG. This setting is optional and can be disabled. Once the configuration is done, it will be saved and activated on the server. Activating the configuration generates all the TMG rules based on the settings.

2.3 Forefront Threat Management Gateway

TMG, previously known as the Microsoft Internet Security and Acceleration Server, is a Microsoft product that can be used as a firewall, a caching proxy and a remote access gateway among other things. TMG is installed with UAG and does not need separate configuration. UAG utilizes the firewall and networking features to implement all the necessary rules for its operation.

The UAG generates several TMG firewall policy rules when the configuration is activated. UAG also generates the DirectAccess networking rules that handle the NAT64 and DNS64 services detailed in chapter 4.

Since UAG uses the TMG for its own purpose, Microsoft defines the support boundaries for what can be done with the TMG by itself when it is used by UAG. In addition to UAG it can only be used for simple firewall rules to limit access to the UAG server or access to internal servers from the UAG and to publish a handful of applications. The TMG can be used to publish Exchange SMTP/POP/IMAP and their secure equivalents and Office Communications Server. Any other services will not be supported by Microsoft. [6]

3 DirectAccess Configuration

The DirectAccess configuration is split into four main components. Each component must be set up before the DA policies can be generated and activated. The generated policies are detailed in chapter 5. Once the configuration is done, the generated policies can also be saved as a PowerShell script. Windows PowerShell is a command-line shell and scripting language that can be used to execute scripts like the one generated by UAG [7]. The configuration is fairly simple since the wizard's guide takes one through the options and has enough description in the dialogs.

3.1 Clients

DirectAccess Clients are defined by Active Directory security groups. This sets the group policy targets by using the groups in the GPO security filtering. The GPO only has computer configuration definitions so the group should only have AD computer accounts. A new group should be created for this use and the necessary computer accounts should be added to it.

3.2 DirectAccess Server

DA server options assign IP addresses to the Internet-facing and the internal networks. The Internet-facing side needs two consecutive addresses which are used for the main connections and tunneling. The internal address can be IPv4 when ISTAP is used or an IPv6 address if the LAN infrastructure is based on IPv6. If ISATAP is used, a static DNS entry for it has to be added to the corporate DNS. By default the ISATAP name is blocked in DNS queries due to the fact that it could allow malicious users to spoof an ISATAP router and capture the client traffic. This option is set in the GlobalQueryBlockList which can be modified with the dnscmd command line tool on all the authoritative DNS servers. [8]

The next option makes it possible to enable NAT64 and DNS64. Alternatively an external server could be deployed to handle those services. In most cases the integrated services are sufficient. These services are detailed in chapter 4.

The last configurations for the DA server are the authentication options. The root CA that verifies all connecting clients must be set. This has to be set to the same CA that hands the computer certificates for the client workstations. The certificate used for IP-HTTPS is also selected in this dialog. Additionally the IPSec cryptography settings can be modified for the established secure tunnels. One can set whether clients need a PKI smart card or if the computer has to comply with the corporate Network Access Policy. The NAP can be set to require certain updates to be applied before the computer is given access to the LAN. It can also be used to make sure the client computers have working and up- to- date antivirus definitions or other software.

3.3 Infrastructure Servers

The infrastructure server configuration defines the internal network location server URL. One can also validate the NLS site in this dialog to make sure the page is reachable. The next steps create the base for the Network Resolution Policy Table. By default the corporate DNS suffix is added to the table and the NLS site FQDN is excluded from it. One can add more entries here if there are several internal DNS domains that one wants to access through DirectAccess. Also the local name resolution settings are defined here. If a client is unable to get a DNS reply from the corporate server it can be set to fall back to local name resolution, which usually means it will resolve the name through the current Internet connection. The next dialog sets the domain controllers needed for client authentication and optionally any other servers necessary for NAP remediation and other server-client connections.

3.4 Application Servers

The application server configuration can change the authentication and encryption method used between a client and a server. If there are no servers that require special authentication or encryption, one can set the configuration to use the end-to-edge model which terminates the encryption at the UAG. If some servers need the end-to-end authentication and encryption, one can add AD security groups that have these special servers as a member.

4 Name Resolution and Location Awareness

4.1 Name Resolution with DNS64

Since all DirectAccess clients have IPv6 addresses assigned to them, they need some method to communicate with the corporate resources that only have IPv4 addresses. The UAG DNS64 service takes the client's DNS queries and relays them to the internal corporate DNS server. When a client wants to access some application server and does not know the server's IP address, it sends out a DNS query. If the application server supports IPv6 and has an IPv6 address the client can communicate to it without the special DNS64 and NAT64 addresses and UAG returns the actual IPv6 address. If the application server only has an IPv4 address, the UAG DNS64 translates the address into a NAT64 prefixed address and then gives it to the client as illustrated in figure1. [9]

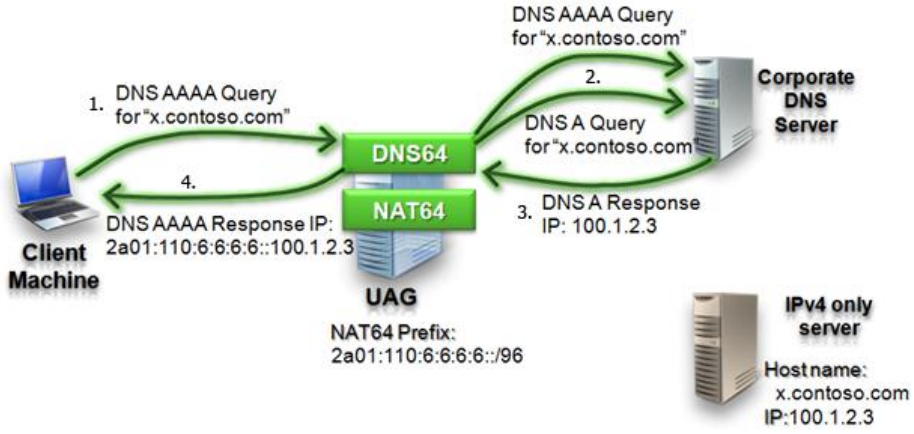

Figure 1. A DNS query through DNS64 [10]

When the client then communicates with the application server, it uses the translated IPv6 address and the NAT64 service on the UAG translates the packet information between them. Figure 2 depicts the packets and their target IP addresses. The NAT64 prefix is configurable but the UAG sets it automatically to a reasonable network. [9]

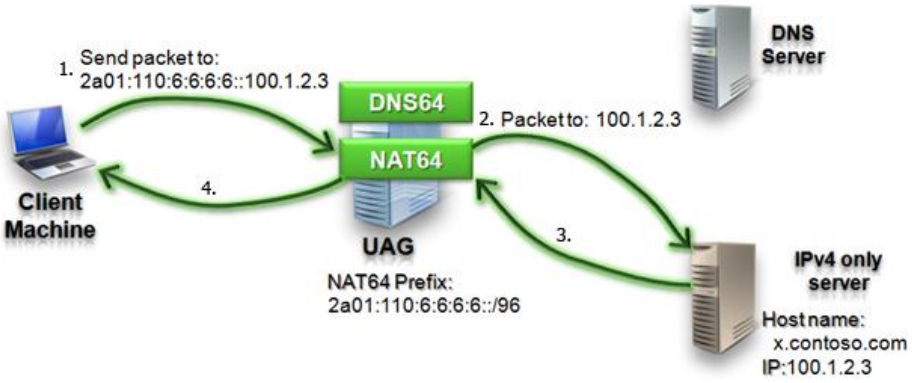

Figure 2. Client traffic with NAT64 translation [10]

4.2 Name Resolution Policy Table

The NRPT makes it possible to direct specified DNS queries to the corporate DNS servers. DirectAccess group policies define the corporate suffixes that are resolved through the DA tunnel from the corporate DNS server. The policies also need to exclude some entries like the NLS which has to be checked through the internet connection to get an accurate result.

The NRPT is generated in the UAG DirectAccess configuration console. The generated table can be modified with the group policy management console, but any custom changes will be lost if the policy is recreated by the DA configuration.

Since the normal Internet access of the DA clients is not routed through the UAG, the NRPT can also be used to define a proxy for some DNS prefix or FQDN addresses. This way the client could access some Internet resources with the corporate public IP address which might be used by some web services to authenticate clients. [11]

4.3 Network Location Server

The NLS is a simple website that is used by clients to determine if they are locally connected to the corporate network or not. The clients try to access the URL defined in their group policy, which is described in more detail in the next chapter. The NLS site is located in the corporate LAN and only responds to requests from the same network. It is common to add a static DNS entry in the corporate domain for the NLS. When the name is only resolvable from LAN, the clients can check their location more easily.

The page does not need any special content as long as the client gets an http response, which means it received the page. Clients check for the NLS page constantly and if they find it, any active DA tunnels can be closed. Similarly if a computer is taken off the corporate network and loses the connection to the NLS, it will know it has to establish the DA tunnel.

5 Active Directory Group Policy Objects

5.1 Client Group Policy

The Client group policy is applied to the DA client computers. It defines several firewall security settings, tunnel properties and rules. It is generated by the DA configuration. This policy also defines the NRPT, which is described in more detail in chapter 4. By default the table includes the corporate network suffix and excludes the NLS. It can be used to add custom proxy rules based on the target hostname or additional DNS server that the client needs to query.

The Network Connectivity Status Indicator settings are also set in this policy. The NLS address is defined as the Domain Location Determination URL. The policy also defines the IPv6 Transition Technologies. It sets the UAG public IP address as the 6to4 relay and the Teredo server and sets the IP-HTTPS URL.

5.2 DaServer Group Policy

The DaServer group policy is applied to the UAG servers. It defines several firewall security settings and tunnel properties. It is generated by the DA configuration.

The policy includes settings for the Clients Access Enabling Tunnel and Clients Corp Tunnel. It defines the local CA that can validate the computer certificates used by the client workstations and the Kerberos and NTLM user authentication protocols. It also details the key exchange and encryption parameters for the tunnels.

5.3 AppServer Group Policy

The AppServer group policy defines another endpoint prefix it can use to create the end-to-end tunnels. In this mode the encrypted tunnel is terminated at the application server and not on the UAG. The policy is filtered to only apply to the security groups set in the DirectAccess configuration. It also makes it possible to change the IPsec properties of the tunnels.

5.4 Firewall Rules Policy

For Teredo functionality the ICMPv4 and ICMPv6 protocols must be allowed between the clients and the UAG server [12]. It allows the client to send ping packets to determine its connectivity and NAT configuration. Enabling the ICMP protocol is also good for troubleshooting. With the ping utility an administrator can easily check if packets are routable between the host and a target computer.

5.5 Computer Certificate Auto Enroll Policy

If the workstations do not have a computer certificate, they must get one from the Certificate Authority. This group policy makes all computers automatically enroll for a computer certificate from the CA. The computer certificate is described in the next chapter.

6 Certificates

6.1 Web Server Template

For the Web Server certificate template we can use the default Web server template as a base and duplicate it to a Windows Server 2008 version, which supports some advanced properties. It will be used for the IP-HTTPS site that the clients use as an IPv6 transitional gateway. This certificate can be issued by the corporate CA so a public certificate is not necessary.

6.2 Computer Certificate Template

The computer certificate template is available on a basic CA installation. The only modification is done to the permissions to allow all workstations to request a certificate for themselves. This certificate is used by the workstations to authenticate with the UAG before the user logs in if a network connection is already established. The computers are forced to enroll for a certificate by a group policy. Only the DirectAccess clients need this certificate.

6.3 Certificate Revocation List

The Certificate Authority is defined to publish the CRL lists to certain locations. Normally the CRL is only published to LAN, but since the client computers cannot retrieve the list before they are connected with DirectAccess they must have access to the list through the internet. This can be accomplished by publishing the CRL and delta CRL to some server which can serve the files to the clients through IIS, for example.

The CRL has a list of the serials of revoked certificates. This information is necessary to properly verify the certificates used by UAG. The CRL also has the CAs Key Identifier so the client can verify that the CRL is actually published by the CA. The CRL also defines the location of the delta CRL. The delta CRL includes all certificates that have been revoked after the publishing of the base CRL. When a client gets a new delta CRL, it combines the list with the base CRL and checks the complete list.

A CRL distribution point must be available on LAN as well so that the NLS site can properly be verified. The CRLs are also used for the IP-HTTPS connections. If the CRL check fails DirectAccess clients cannot make IP-HTTPS connections. [13]

7 Conclusions

DirectAccess is a very simple way for the end users to gain access to the corporate resources. They need not establish the DA connection once they get connected to the Internet since it's done automatically. The configuration has several steps, but they are fairly well documented in the Microsoft TechNet library now that the UAG has been released.

This configuration was used as a base when testing in a virtual environment and was actually implemented on a few existing infrastructures. The main components necessary for this testing were the DC, a UAG server and a Windows 7 client. For proper tests another server was added to the LAN to check how the client accesses it through DA. In a virtual environment it is easy to separate the LAN and DMZ networks so the client computer can be moved around between the networks to see its behavior. In the virtual lab environment the network traffic was also inspected with a network protocol analyzer which did not show much information since the actual traffic is encrypted. Once the ISAKMP key exchange was done the traffic was basically only IPv6 packets with ESP.

It was noted that the NRPT is very fragile and can get easily corrupted when edited through the group policy editor. A few times during pilot testing there were extra entries in the table that prevented the NLS from working properly leading to a complete loss of local network connectivity. Once the table has been corrupted and the client cannot reload the configuration from the network, it has to be manually corrected from the computer's registry with the Registry Editor.

This study was limited to a simple DA implementation and did not cover any special PKI features like a smart card that could have been used for user authentication. It also did not implement any network access protection, which should be one of the main concerns with letting computers access the network from the outside. A proper NAP check should be done before the client is given access to any critical systems.

In the future it would be interesting to test the deployment of multiple UAG servers in some array configuration. Also a load balanced configuration might be reasonable in a larger environment. What kind of balancing would be the best, a simple round-robin or a more advanced type of

selection based on the client's location or resource needs? A proper IPv6 infrastructure would not need all the transitional technologies and the DA might be slightly easier to implement in such an environment.

References

1 Microsoft TechNet: Resources for IT Professionals, 19 April 2010. URL:http://technet.microsoft.com. Accessed 19 April 2010.

2 TechNet Blogs – Blogs, 19 April 2010. URL:http://blogs.technet.com/. Accessed 19 April 2010.

3 Microsoft Forefront: Overview, 19 April 2010 URL:http://www.microsoft.com/forefront/en/us/overview.aspx. Accessed 19 April 2010.

4 System requirements for Forefront UAG servers. 19 April 2010. URL:http://technet.microsoft.com/en-us/library/dd903051.aspx. Accessed 19 April 2010.

5 DireactAccess Requirements and Prerequisites, 19 April 2010. URL:http://technet.microsoft.com/en-us/library/dd637780%28WS.10%29.aspx. Accessed 19 April 2010.

6 UAG Support boundaries, 19 April 2010. URL:http://technet.microsoft.com/en-us/library/ee522953.aspx. Accessed 19 April 2010.

7 Windows Server 2008 R2: Server Management, 19 April 2010. URL:http://www.microsoft.com/windowsserver2008/en/us/server-management.aspx. Accessed 19 April 2010.

8 Windows Server 2008 Technical Overviews, 19 April 2010. URL:http://www.microsoft.com/downloads/details.aspx?familyid=46dc26d6-af47-43f0-b3de-521831fe09d6&displaylang=en, DNS_Server_Global_ Query_Block List.doc. Accessed 19 April 2010.

9 Deep Dive Into DirectAccess – NAT64 and DNS64 In Action, 19 April 2010. URL:http://blogs.technet.com/edgeaccessblog/archive/2009/09/08/deep-dive-into-directaccess-nat64-and-dns64-in-action.aspx. Accessed 19 April 2010.

10 NAT64 and DNS64, 19 April 2010. URL:http://blogs.technet.com/edgeaccessblog/archive/2009/09/08/deep-dive-into-directaccess-nat64-and-dns64-in-action.aspx. Accessed 19 April 2010.

11 DirectAccess Connectivity, 19 April 2010. URL:http://technet.microsoft.com/en-us/library/dd637795%28WS.10%29.aspx. Accessed 19 April 2010.

12 UAG Domain Controller configuration, 19 April 2010. URL:http://technet.microsoft.com/en-us/library/ee861152.aspx. Accessed 19 April 2010.

13 Designing your PKI for Forefront UAG DirectAccess, 19 April 2010. URL:http://technet.microsoft.com/en-us/library/ee406213.aspx. Accessed 19 April 2010.