Jyri Ahonen

Replacing VPN connections with DirectAccess connection

Metropolia University of Applies Sciences
Bachelor of Engineering
Information Technology
Bachelor's Thesis
May 16, 2012

Author Title	Jyri Ahonen Replacing VPN connections with DirectAccess connection
Number of Pages Date	28 pages May 16, 2012
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Telecommunications and Data Networks
Instructors	Niko Ronkainen, IT Specialist Erik Pätynen, Senior Lecturer

The aim of this thesis was to find out if DirectAccess remote access solution can be used to replace the company's current VPN remote access solution which has served for some years now, what additional benefits the solution would provide, and how it can be implemented into the existing network infrastructure. The objective of this study is to provide user friendly remote access for the remote users, which would work over all different network solutions and which would provide secure and effortless connection into the company's internal resources. On the other hand, one of the aspects of the study is to determine what kind of remote control possibilities DirectAccess would provide for the IT department, whose aim would be to get the machines that are rarely connected into company's internal network, under remote management.

The research on DirectAccess remote access compatibility and functionality was done based on web pages that were considered reliable, in practice relaying on Microsoft's own TechNet and TechNet Blogs web pages. Microsoft Forefront Unified Access Gateway SP1 was chosen to provide Direct Access remote access solution, which includes integrated transition technologies that allow sharing of services and functions behind IPv4 and NAT networks for remote users, when pure DirectAccess works only over IPv6 networks.

Microsoft Forefront Unified Access Gateway SP1 was installed on the test server and it was configured to provide remote access into internal network services from the external network. The study describes the installation and configuration steps that were done as well as explains what other servers may be needed to create a large-scale environment. Establishing the remote connection, its operation and security were tested by connecting into internal network resources using the Direct Access remote access in actual everyday work.

In conclusion, the upcoming Windows Server 2012 Direct Access remote access solution and its new features compared to the current Microsoft Forefront Unified Access Gateway 2010 solution is reviewed.

Keywords	DA, DirectAccess, UAG, remote access

Tekijä Otsikko Sivumäärä Aika	Jyri Ahonen VPN yhteyksien korvaaminen DirectAccess yhteyksillä 28 sivua 16.05.2012
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaajat	IT Asiantuntija Niko Ronkainen Lehtori Erik Pätynen

Tämän insinöörityön tavoitteena oli selvittää sopisiko DirectAccess etäyhteysratkaisu korvaamaan yrityksen nykyisen jo joitakin vuosia palvelleen VPN etäyhteyden, mitä lisähyötyjä ratkaisu tarjoaisi ja kuinka se sopisi asennettavaksi osaksi nykyistä verkko infrastruktuuria. Tutkimus tehtiin tavoitteena tarjota yrityksen työntekijöille mahdollisimman helppokäyttöinen etäyhteys, joka toimisi kaikkien erilaisten verkkoratkaisujen yli mahdollistaen turvallisen ja vaivattoman yhteyden yrityksen sisäisiin resursseihin. Toisaalta yksi tutkimuksen näkökannoista oli selvittää minkälaiset etähallinta mahdollisuudet DirectAccess tarjoaa IT-osastolle jonka tavoitteissa olisi saada harvoin yrityksen sisäverkkoon yhteydessä olevat koneet etähallinnan piiriin.

Tutkimustyö DirectAccess etäyhteyden soveltuvuudesta ja toiminnallisuudesta tehtiin luotettavina pidettäviin, käytännössä Microsoftin omiin TechNet ja TechNet Blogs verkkosivuihin pohjautuen. DirectAccess etäyhteys ratkaisuksi valittiin Microsoft Forefront Unified Access Gateway SP1, johon on sisällytetty useita käännösteknologioita, joiden avulla IPv4- ja NAT-verkkojen takana olevat palvelut ja toiminnot saadaan jaettua etäkäyttäjille, muuten vain IPv6 yhteyksillä toimivan DirectAccess-etäyhteyden yli.

Microsoft Forefront Unified Access Gateway SP1 asennettiin testipalvelimelle ja konfiguroitiin tarjoamaan etäyhteys ulkoverkosta sisäverkon palveluihin. Työssä kuvataan kaikki asennuksessa ja konfiguroinnissa läpi käydyt työvaiheet sekä selvitetään mitä muita palvelimia mahdollisesti tarvitaan laajamittaisen ympäristön luonnissa. Etäyhteyden muodostumista, toimivuutta ja tietoturvaa testattiin käyttämällä DirectAccess etäyhteyden yli sisäverkon resursseja normaalissa työkäytössä.

Lopuksi tarkastellaan tulossa olevan Windows Server 2012 tarjoaman Direct Access etäyhteys ratkaisun tuomia uusia ominaisuuksia, verrattuna nykyiseen Microsoft Forefront Unified Access Gateway 2010 ratkaisuun ja päätetään jatkotoimenpiteistä.

Avainsanat DA, DirectAccess, UAG, etäyhteys

Contents

Abbreviations

6to4	System that allows IPv6 packets to be transmitted over an IPv4 network
AD	Active Directory
CA	Certificate Authority
CRL	Certificate Revocation List
DA	DirectAccess
DC	Domain Controller
DCA	DirectAccess Connectivity Assistant
DCOM	Distributed Component Object Model
DMZ	Demilitarized Zone
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
GPO	Group Policy Object
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
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
NIC	Network Interface Controller
NLS	Network Location Server
NRPT	Name Resolution Policy Table
PKI	Public Key Infrastructure
Teredo	IPv6 connectivity over IPv4 without native IPv6 network
TMG	Microsoft Forefront Threat Management Gateway
UAG	Microsoft Forefront Unified Access Gateway
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WFAS	Windows Firewall with Advanced Security

1 Introduction

This thesis is made for Tekla Oyj, multi-national software company, whose employees need to get reliable access to many different internal services which are located at multiple sites all around the world.

This thesis researches the possibility to change existing VPN solution with Microsoft Direct-Access remote access solution, what benefits it would produce and how to implement it into existing environment.

The research is made to find out what benefits DirectAccess would provide for mobile users using company's resources with remote access over insecure networks, compared to existing VPN solution. It also focuses on finding out what benefits DirectAccess would provide, such as improved manageability of remote users and for IT department up-keeping mobile users computers which are connected to the corporation's internal network on rare occasions.

> Microsoft DirectAccess is a feature in the Windows 7 and Windows Server 2008 R2 operating systems that gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess, users are able to access corporate resources (such as e-mail servers, shared folders, or intranet web sites) following common security standards, any time they have an internet connection. [1.]

This thesis describes the prerequisites for implementing Microsoft DirectAccess to existing corporate environment which already contains Microsoft Windows Active Directory infrastructure and multi-site network infrastructure including firewalls, network acceleration, DNS and other multi-site services. The corporation's resources also cover existing Windows 7 workstations and Windows Server 2008 R2 servers.

Research for this thesis is made relying on comprehensive documentation of DirectAccess and Microsoft Forefront Unified Access Gateway at Microsoft's TechNet [2] and its blogs [3], and on other internet sites and blogs which are considered to be reliable. Tremendous amounts of information can be found about DirectAccess and UAG from several sites on the internet. There are specific descriptions of the technologies behind DirectAccess solution which can be used to help you to select the best settings for your environment. There are also many blogs and forums where you can find many real life situations that can be helpful for finding information when troubleshooting your DirectAccess infrastructure.

For implementing the DirectAccess solution, Microsoft Forefront Unified Access Gateway (UAG) Service Pack 1 (SP1) is selected, for its integrated transition technologies such as 6to4 and Teredo to traverse the IPv4 Internet or NAT networks and for unified management and control over the DirectAccess solution with UAG DirectAccess arrays.

After the UAG solution is selected, we go through all prerequisites needed to successfully implement it into existing environment and what changes are needed to the existing services. After prerequisites are reviewed, a test server is set up and UAG is installed into it. Making the installation and configurations are described step by step, and all management options are checked out in order to figure out all variables that can affect the deployment.

In the end this study is made to find out if the current VPN connections can be replaced with DirectAccess connection, so after testing period we went through issues for and against the change, and tried to figure out if the current UAG DirectAccess version is ready to be implemented into existing environment.

2 Direct Access Implemented with UAG SP1

2.1 DirectAccess

DirectAccess (DA) is a new feature which was released in Windows Server 2008 R2 and Windows 7 operating systems. With DA mobile users can access the corporation's internal resources with encrypted connection without using virtual private network (VPN). DA creates two way tunnels to DA client computers whenever the computer is connected to internet, even before the user logs into the computer. DA creates an infrastructure tunnel, which can be used by IT administrators to manage out DA client computers every time the computer connects to common internet. This creates seamless connection for users to access the corporation's resources without any user action needed.

While DA itself is included in the operating systems, Microsoft has also created Forefront Unified Access Gateway (UAG) 2010 [4], software package that eases up DA configuration, adds many features to DA and includes many transition techniques needed to install DA into environments that are not fully implemented with IPv6. Of course other services can be used to expand DA's usability and other transition mechanisms like NAT-PT [5] can be used to make DA to work over IPv4 networks, but this study does not cover those subjects.

2.2 Forefront Unified Access Gateway (UAG) Service Pack 1 (SP1)

DirectAccess solution is implemented with Forefront Unified Access Gateway (UAG) Service Pack 1 (SP1) which will provide many improvements to regular DirectAccess solution that is included in the operating systems. In addition to DirectAccess, UAG offers integrated transition technologies such as 6to4 and Teredo, which are needed to provide connectivity over current IPv4 and NAT network infrastructure, improved configuration wizards, which makes installation much easier compared to power shell scripts, simplified configuration of the connectivity assistant and easier configuration of ”manage out” deployments. UAG also offers unified management and control over the DirectAccess solution with UAG DirectAccess arrays, which are intended to be used in the company-wide deployment.

UAG SP1 was chosen for this installation because of its many advantages over DA, like better manageability and scalability, and also for its new features like NAP health policies and logging and monitoring.

2.3 Prerequisites for UAG

To successfully implement DirectAccess solution, there are many different aspects that need to be considered. In addition to normal hardware and software requirements there are plenty of other criteria which need to be satisfied, such as requirements for other servers and sites, different connections for many different transition technologies in use and the need of multiple certificates. [6.]

Hardware requirements for the DA server are fairly easy to fulfil, including a modern dual core processor, 8GB of memory and two network adapters. Software prerequisites can also be quite easily met, when the corporation already have their DC, DNS and other servers involved running Windows Server 2008 R2 and mobile client computers are running Windows 7 Enterprise. Clients must be members of an Active Directory domain [7], but this requirement is probably not a problem for machines you want to give a connection to your internal services. When Microsoft Forefront UAG is chosen for DA solution it also covers all transition software needed for legacy connectivity over IPv4 network.

IPv6 issues require a more extensive survey, when servers providing services to DA clients need to be connectible with IPv6 and client applications must be IPv6 aware. Of course IPv6 also brings challenges to existing network infrastructure including existing network acceleration and firewall hardware.

DA needs highly available network location server (NLS) [8], which must be in the corporations network and that is assigned with valid web site certificate. Internal PKI is needed to assign machine certificates to DA clients and the DA server. Availability of other services is important for DA functionality but if ISATAP [9] is used, DA server's availability is crucial for other servers network communication, since it is acting as discovery service for IPv6 traffic.

3 Implementing Direct Access into Existing Environment

3.1 Placement of Servers

DA server provides connection from the internet to the internal network for DA clients, so the server needs to be connected directly to both networks and this prevents usage of NAT or any other functionalities normally used to provide network security. Server can be installed into DMZ or like in this case, to the perimeter network, between internet-facing firewall and intranet, as shown in Figure 1. [10.]

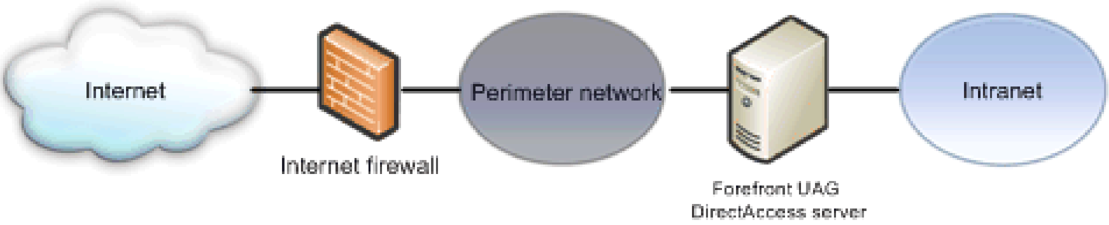

Figure 1. Where to place the Forefront UAG DirectAccess server [11.]

When the UAG server is located behind the company's perimeter firewall, you need to configure some new rules to allow inbound traffic for both of the servers external IPs. These new configurations are made for three different connection types that DA uses: 6TO4, Teredo and IP-HTTPS. DA establishes connections through these different connection types, depending on the network you are connecting from, and on the network where to the connection is made, so basically you need to provide them all.

3.2 Firewall & Threat Management Gateway

For DA servers security UAG package provides normal Windows Firewall, which provides basic firewall functionality. UAG also includes Microsoft Forefront Threat Management Gateway 2010 (TMG) [12], which is a single solution integrating multiple layers of web security technologies that provides protection against threats for a secure web gateway.

UAG uses TMG infrastructure and functionality in some scenarios and it is intended to be used without modifications, but UAG DA installation leaves almost everything blocked in the TMG, including ping and Remote Desktop, so you need to modify some rules right away, so that you are able to establish remote connections to the server and test its connections with ICMP echoes. TMG is extensive application, which has significant amount of settings, but there is not much that needs to be done in order to make the DA operational. When UAG server is used to provide VPN connections to the corporation's resources, you should check out TMG configurations thoroughly, because TMG is used to create access rules and it can be used to publish some applications via it. In general DA scenario you just need to be aware that there is another solution running in the background when you make changes to the UAG servers configuration and when you run tests, to confirm that all connections work as they are planned.

3.3 Policies Related to DA

DA clients need to be enabled using either Active Directory Security Group(s) [13] or Active Directory Organizational Unit(s) (OU's) [14], whichever you prefer in your environment. In this case we used security group to include these policies in the existing hierarchy. You can use UAGs configuration wizard to generate three GPOs needed for DA policies, or you can create them manually in order to choose the location where these GPOs are placed in the tree hierarchy. These three GPOs include DA policies for clients, gateway and application servers, which can be applied to the AD Security Group(s) or AD OU(s).

We created a single Security Group which only purpose is to enable DA for the clients, where the members of this group are computer objects, not users. Once you make the computer a member of this group you just need to run Group Policy update or restart the client computer, and the usage of DA is enabled.

3.4 Certificates Related to DA

DA connection requires a couple of different certificates that can be provided through in-house enterprise certificate server or by using 3rd party certificates. You need to have a Public Key Infrastructure (PKI) [15] in place and UAG server needs a Web Server certificate from Certificate Authority (CA) [16] that publishes its Certificate Revocation List (CRL) into external network for the DA clients.

In this installation 3rd party certificates are used to ease the implementation, when existing in-house enterprise certificate server is not connectible from external DNS, and to make sure that DA clients can reach the CRL at all times, because the clients can not establish connections if the certificate can not be trusted.

4 DNS

4.1 Name Resolution

DA makes its clients completely dependent on the DNS to be functional, particularly when there is only Ipv4 network behind the UAG server, which makes it act as an Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) router.

4.2 External & Internal DNS

DA clients create tunnels from external network into the UAG server, so its (first) external IP address needs to be added to your external DNS. The name used in external DNS does not matter because it is only used internally by the program when client and server negotiates establishing IP-HTTPS interface [17], you just need to remember to use the same name when you create the IP-HTTPS certificate.

Only your domain members use this IP-HTTPS certificate, so it does not have to be issued by 3rd party CA, but it needs to be available through the external DNS, so that the clients can always reach the CRL for the certificate. DA uses IP-HTTPS tunnels when it establishes infrastructure tunnel to the client, therefore the availability of the certificate is vital to the functioning of the service.

At the internal side, Windows Domain typically allows DNS clients to dynamically update their records, which normally makes usage easier, but it also provides a way to alter DNS records in unwanted ways. To reduce the risks Windows Server DNS uses ”Global Query Block List” which blocks some of the more vulnerable protocols by default, like ISATAP. In the environment in question ISATAP needs to be enabled if UAG is configured as it is designed to work with IPv4 network.

4.3 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)

Currently significant amount of companies' network infrastructures are implemented with IPv4. In order to get DA to work, UAG server needs to act as an ISATAP router which translates traffic in both directions, IPv6 into IPv4 and IPv4 into IPv6, when all communication between DA server and DA client is established in IPv6 only. For this purpose UAG DA installation includes Network Address Translation64 (NAT64) and Domain Name System64 (DNS64) functionalities [18], which perform Ipv6-to-IPv4 DNS name resolution and Ipv6/IPv4 traffic translation services. With these features DA allows clients to communicate with host by ISATAP derived global addresses and provides ISATAP router to tunnel packets through the existing IPv4 infrastructure.

When ISATAP is used and all traffic is translated on the way, this can cause problems in some applications, which are designed to work in direct connection with the services server or that are using their own non-standard protocol to communicate. There are known problems at least with SAP, Microsoft's Office Communicator and VOIP solutions in general, so before you can rely on DA as your only remote working solution, you need to map and test thoroughly all applications used in your company.

UAG server acting as ISATAP router in the network allows all Ipv6 enabled devices, like all computers running with recent Windows version to establish Ipv6 connections through it, which can be problematic when all applications do not support IPv6. Windows Server 2008 R2, Vista and Windows 7 are built to prefer IPv6 and when IPv6 is preferred these computers start to respond to pings and other traffic from IPv6 addresses, so the behaviour of the whole network changes. If this change is allowed in the network, UAG server's role becomes crucial and its availability needs to be re-evaluated.

5 Servers Providing Services to DA Clients

5.1 Network Location Server (NLS)

There are many servers that need to be configured to work with DA, like AD and DNS, which usually already exists in the corporate environment, but DA requires also Network Location Server (NLS) in order for it to work. NLS is in key role for DA clients, because it is used to determine when the client is connected into internal network and when it is at the external network and needs to create DA tunnel to reach internal resources.

NLS used in the DA configuration is an HTTPS site which needs only to respond to HTTPS request through internal DNS. Basically it can be any highly available site which is certificated with its fully qualified domain name including also the domain name, not just with the host name because configuration does not accept that, and its name can only be resolved when client is connected to internal network.

For NLS usage, you can create a new site into existing Internet Information Services (IIS) server, or even stand up new IIS server for NLS, but this is not really necessary because there is not much traffic to the site. You can easily use an already existing site for this purpose, even though all Microsoft's instructions tell you that you need to create new one. Using an existing site also saves you from adding this new host URL into your internal DNS and prevents the need to grant a certificate for the new host name.

The only real concern for the NLS site is its high availability, because its connection is the only way for the client to determine if it needs to establish DA tunnel. If the NLS site is unreachable, all DA clients will tunnel all their internal network traffic through UAG server also when they are inside the corporation's network.

5.2 Generally

In order to make DA configuration complete, you also need to do add some new configurations or do some changes to other servers that are used with DA. You need to do changes into DNS servers of your environment, external DNS needs to be updated with UAG servers name so that clients can connect to it from the internet and internal DNS needs to be configured to allow ISATAP if it is used in your configuration.

DA configuration creates, or reconfigures GPOs which are located at AD, so there is no need to do any modifications to those at AD side, but at the AD you need to add client computers into the Security Group, which enables DA usage. You also need AD to add UAG server and DA clients as Domain members.

In the best case scenario, servers providing services that are used by DA clients, do not need to be altered. When everything is working as Microsoft has planned it to work, UAG should take care of network translation if needed, and all services should work right away. Of course this is not always the case and there are some configuration changes that need to be done in some systems, in order to get them to work, but sometimes even the configuration changes will not help, so all services can not be used through DA.

6 Configuring DirectAccess

6.1 DirectAccess Server

First we set up a test server, which meets the requirements described in the prerequisites. The server was set up in a virtual machine, and when DA is taken into live usage, the actual server is also installed into virtual environment, so its features can be altered quite easily in the future in case of any performance issues, when DA usage starts in full scale. Windows Server 2008 R2 Standard was installed into the server, when there was no benefit in installing any extended version into UAG usage. After OS installation, the server was installed with additional programs, defined by company's policies and it was added into domain.

The server was placed into the perimeter network, between internet facing firewall and intranet, where it is secured behind the corporation's hardware firewall and it can access all internal resources, that can be used through DA. The two network interface controllers were assigned with static IPs, which were reserved from the corporation's addressing pool. The internal network interface does not get the default gateway information, so you need to add all subnets you want to get connected through DA with persistent static routes.

Firewall is configured to block all undefined connections so some adjustment is needed for UAG servers connectivity. Protocol 41 was allowed for 6TO4 connections, UDP traffic to port 3544 was allowed for Teredo connections and TCP traffic for port 443 was allowed for IP-HTTPS connections. These changes are the least you need to do, but you might also want to allow some other traffic, like ICMP echoes, for testing and troubleshooting with ping requests.

6.2 DirectAccess

Forefront Unified Access Gateway (UAG) Service Pack 1 (SP1) was installed into the server for DA solution. UAG installation is very easy [19], but it installs many components, like Forefront Threat Management Gateway, SQL Server 2008 and UAG itself, so it takes a while. SQL Server 2008 is included in installation for UAGs own logging, so there is no need for database administration. Once the UAG installation is finished, you should take some time to check that latest updates are installed for all components in the solution.

After installations we did some changes into TMG, which has everything blocked as default, as it should, but for the ease of use we allowed remote management and ping into the server from some internal network subnets. Another modification we configured into TMG was to allow UAG server to connect into the in-house certificate server, otherwise certificate renewals would fail.

DA needs Public Key Infrastructure (PKI) for it to work, and it is mandatory, so you need to install certificate server if you do not have one. In this installation we used already existing PKI for internal certificates, so we only needed to enable certificate enrollment from the UAG server. After enabling enrollment, you can request certificates, which can be easily done with Certificate Enrollment Wizard, if your UAG server is allowed to connect to the DCs with Distributed Component Object Model (DCOM), which is *Microsoft technology for communicating among software components* [20].

UAG server also needs Web Server certificate, which CRL needs to be published to external network for the DA clients. For the test installation we acquired test certificate from 3rd party CA VeriSign (which was acquired by Symantec during this thesis) which worked very well for this purpose. This certificate generated by VeriSign was then imported to UAG server's Computer Account Personal Certificate store. High availability needed for CRL and the fact that it needs to be published on external network speaks on behalf of 3rd party CA, but just as well you can create your own certificate and publish it, when all computers that are using it are DA clients, which are your domain members that trust your internal CA.

For DA configuration we created AD security group for enabling DA clients, and three GPOs for DA policies, in order to get them where we wanted them in tree hierarchy, because if you do not create them beforehand, configuration creates these GPOs into the Active Directory.

The next step in DA configuration was to open the UAGs “Getting Started” wizard, which guides you through configuring all necessary settings. At first the wizard goes through configuring network settings, ensuring that your two NICs are connected to correct interfaces and that your static routes reach all wanted subnets. The next step goes through server topology, where single server installation was chosen in this case. It is quite obvious to start with single server installation, when you can later deploy other UAG servers and create the array, when you have first made everything work at the “Master”-server. The last step is just about enabling Windows update and about participating in the Customer Experience Improvement Program. After the wizard we activated the configuration, even though the configuration was far from complete, this allowed us to get the first backup from the configuration.

After “Getting Started” wizard you get to the UAG Management, where you can find four different steps, which all are used to configure some specific part of the UAG configuration. The first step is about clients and GPOs configuration, and the first option is the deployment model, where you can choose if the DA is used to provide the corporation's resources, or if the DA is only used to “Manage Out” the client computers. Also the option providing the corporation's resources involve the infrastructure tunnels which are used to connect to client computer from internal network, so DA clients can be always managed when it is connected to internet. The second setting is for selecting domains that are allowed to be connected by DA clients. The last two settings are for selecting GPOs and the AD security group, that were created before.

Optional setting for the first step is for DA Connectivity Assistant (DCA) configuration, where you can set some options for troubleshooting the connectivity. At first you set the DCA on and choose if you want to allow the clients to use external DNS when the DA connection is not working. Next you set resources against which to check if the connection is working or not. The resources can be network shared files, or HTTP / HTTPS sites, which can be connectible only when the client is connected to internal network. The third option is for setting help site, where clients can find out instructions or contact information when the connection is not operational. The last option is for setting email address where troubleshooting logs are sent, and to set additional scripts to be run on client. Results of the scripts are sent alongside the default logs to the specified email address.

Step two is for configuring DA server settings, and it covers network connectivity, IP-HTTPS Certificate and Ipsec CA configurations, as well as a number of optional settings. First you select the correct IP addresses for the interfaces, and if you have configured them correctly before, you should only have one option where to choose from. The second setting is for browsing the Web Server certificate and the CA issuing it. The last setting is for defining the internal CA that issues the Computer Certificates for the DA clients. Optional settings covers Two-Factor Authentication which we did not enable at least at this point, Network Access Protection (NAP) configuration which was not enabled at this point either, Force Tunneling configuration which was left to Split tunneling setting so that all clients internet traffic is not routed through UAG server. The last option is for Server Groups configuration which was not used at this stage, in the single server topology.

UAG provides the possibility to use NAP, which is Microsoft's protocol for checking the clients health before letting it connect into internal network, and its Health Registration Authority (HRA) [21] and Network Policy Server (NPS) [22] components are installed automatically during UAG installation. You can use other HRA or NPS component for NAP, but these components that are included into UAG provide basic checks, to verify that the client has its firewall, anti-virus and security updates etc. on, are usually enough, so in order to get working NAP you just need to configure CA to issue health certificates for UAG.

The third step is for configuring Infrastructure Servers, where you specify which servers the computer can connect to before user has logged in and which servers can not be connected through DA, like NLS. NLS configuration is the first option, where you specify the Fully Qualified Domain Name (FQDN) and validate that the NLS site you chose is working with the DA configuration. The second option is for DNS suffixes where you can specify DNS names and patterns inserted to DA clients Name Resolution Policy Table (NRPT), but there was no need to specify these, when the corporation's internal and external domain names differ from each other and the two items that need to be always in the list, windows domain and NLS, are filled in automatically. Here you should also exclude domains providing services to the internet, like webmail and interfaces providing VOIP connections. The last page of this step is where you configure management servers where the client can connect through "Infrastructure

Tunnel”, like DCs, antivirus servers and other servers that provide software updates to the clients. Configuration found almost all management servers and we only needed to add servers providing Windows updates. After everything is set, these settings are applied to the client GPO.

The last step is called End-to-End Access and it is used to configure where the DAs encrypted tunnel is decrypted. In the default setting “End-to-Edge”, traffic from client to UAG server is always encrypted, but if you want, you can set the connection to be “End-to-End” where encryption goes through UAG server all the way to the connected server. In this installation we used default setting, when the corporation's network is providing its own security capabilities so there was no need for extra encryption.

When all the steps are configured and optional settings are set, you need to apply policies and then activate the configuration. When you apply policies, UAG generates GPOs and applies all given parameters and settings into them, by executing a powershell script. These new GPOs are distributed into clients by manually running group policy update or when the client computer is restarted. After applying policies you need to activate configuration to get the new settings that are not in the GPOs, into use. During activation you are prompted to backup the configuration, like at the first time after “Getting Started” wizard. Every time you make changes to UAG configuration you need to remember to apply policies and to activate configuration to get the changes to take effect.

6.3 DirectAccess Clients

DA clients do not have any specific hardware requirements, that are required to get DA working, but rather new hardware is recommended when all traffic through DA is encrypted, two times even in some cases, so computing power is needed in order to get pleasant user experience.

The only real requirement for DA, besides that the client computer needs to be a domain member, is that the client computer is running Windows 7, Enterprise or Ultimate version, or Windows Server 2008 R2. Other Windows OS versions or other OSs can only be made to work through UAGs SSL VPN add-on, which is not implemented in this scenario.

When DA client meets requirements described above and it is added to AD security group, which enables DA usage, there are no configuration changes needed, not even to clients firewall. DA uses Windows Firewall with Advanced Security (WFAS) policies to enable required protocols between the DA client and server. UAG wizard creates this GPO used to enable DA, and these GPO settings include the WFAS policies that alter the clients firewall settings.

Client connectivity can be monitored with DA Connectivity Assistant (DCA), which is not installed to the client as default. It can be installed if needed, or you can create separate application deployment policy which can be used to deploy it to all clients. DCA runs as system tray balloon, which always indicates the status of "Corporate Connectivity" for the user. DCA also provides "Troubleshooting Portal" that can be used to gather and send predefined information for IT administrators, or to open help site, that you have defined to help users in connectivity issues.

6.4 Servers and Services Used with DA Installation

There are several servers that are normally used as part of the DA environment, but Domain Controller is the only other mandatory server in DA environment, in addition to the DA server itself. DC is needed for AD security groups, GPOs and for getting the client added into the domain. In typical installation DNS, CA and NLS are located at separate servers, which are then updated or changed to provide services for UAG server and UAG configuration is defined with the information about these servers.

Then there are two different kind of servers, those that are used through DA connection and those that are providing services for the clients through infrastructure tunnels. The servers that are used through DA do not need any configuring into UAG, the only exception being if you want to prevent connection into some internal resource, UAG needs to be configured with the name of that kind of host. Infrastructure servers are also added to UAGs configuration only by host name, there is no need to set complex settings.

7 Results

The corporation's mobile users need a way to get remote access into the corporation's resources and DA offers a very easy way to provide this connection. DA solution used in this installation was UAG which has been on the market for a couple of years so there were very comprehensive installation and configuration instructions at the Microsoft's TechNet and other websites. UAG turned out to be very easy to install and configure, so we could easily test different configurations and connection scenarios.

DA client establishes connection to DA whenever the computer is connected to the internet, even before the user logs into the computer, so end users do not need to manually establish a VPN connection. In tests this turned out to work in general as promised and connection was established automatically when the computer was connected to external network. In the best cases DA feature established connection very quickly and recognized network change between internal and external networks within seconds. However, there were a couple of times when connection status change took nearly one minute, and this can confuse the end user, if there is no clear status indicator about what is happening, so the installation of DCA is almost mandatory.

UAG was installed into test server, but the server was connected into the corporation's live network to test how everything works in actual everyday work, with couple of test laptops, so that environment changes do not affect more than these test laptops. Tests confirm that DA is a very easy and convenient remote connection into systems that agreed to work with it. There were a couple of applications that did not want to co-operate through DA but we had restricted possibilities to troubleshoot production applications. Production environment was left untouched in these tests, so it is uncertain if these applications could be made to work through configuration changes.

All the systems that worked with DA were working without any modifications and they worked with both tested scenarios, through ISATAP and 6TO4 connections. Both scenarios include translation between IPv4 and IPv6 protocols, when all operated servers were using IPv4 network connections. When connection always includes IPv6 protocol, it makes troubleshooting more difficult, when you can not use the tools that you are used to, like ping and nslookup. You should also note that investigating the traffic from the application servers end, it only sees the decrypted traffic coming from the UAG server.

When remote management functionalities were investigated, it was found out that security updates were not successfully deployed over infrastructure connection, as they are at present if remote user uses VPN connection. This was a big disappointment when security and health policy issues were meant to be upgraded from the present solution. Further in the tests NAP functionality was tested with the client computers and its operation was found to correct some of the weaknesses in normal security update functionalities. NAP client is included in Windows OSs and it proved to work reliably and fast. Its client application recognized changes in configuration within seconds and changed connection into infrastructure only, when it detected any breaches of the security laws.

DA is designed to work with IPv6 networks and UAG is created to provide transition technologies into old IPv4 connectible infrastructure, so when all existing infrastructure is in IPv4, the transition technologies get up to the main part of the study. ISATAP was reviewed before in chapter 4.3 and there you can see that there needs to be profound deployment planning before you deploy it into the existing environment, so that the changes in the connections will remain under control.

The UAG installation was made into single server for this test, but the actual need is to install UAG into array with multiple sites. Array installation has not claimed to be an easy task at present, but Microsoft has just released more details about its forthcoming server release Windows Server 2012, where there will be many improvements into the basic DA, which will take it close to present UAGs functionality, and one of those published improvements is to ease up and simplify the array installation and management [23.].

The forthcoming Windows Server 2012 Direct Access will provide almost all present UAGs functionality, basically only lacking TMG, and will bring many improvements into DA functionalities, like multi-site entry point selection based on location and removing the double encryption issue with IP-HTTPS, so it seems to be worth the wait [24.].

The final result of this thesis is that IPv6 network infrastructure and IPv6 aware applications are necessary for DA to work effectively. If DA implementation is not needed right now, you might want to postpone the DA implementation until new technologies can be exploited when the Windows Server 2012 will be released.

References

1 Microsoft. Windows Server 2008 R2 DirectAccess [online].

URL: http://www.microsoft.com/en-us/server-cloud/

windows-server/directaccess.aspx. Accessed 10 May 2012.

2 Microsoft TechNet. Microsoft TechNet [online].

URL: http://technet.microsoft.com/en-gb/. Accessed 10 May 2012.

3 Microsoft TechNet Blogs. Microsoft TechNet Blogs [online].

URL: http://blogs.technet.com/. Accessed 10 May 2012.

4 Microsoft. Forefront Unified Access Gateway 2010 [online].

URL: http://www.microsoft.com/en-us/server-cloud/forefront/

unified-access-gateway.aspx. Accessed 10 May 2012.

5 Wikipedia. IPv6 transition mechanisms [online].

URL: http://en.wikipedia.org/wiki/IPv6_transition_mechanisms. Accessed 10 May 2012.

6 Microsoft TechNet. Forefront UAG DirectAccess prerequisites [online].; 1 February 2011.

URL: http://technet.microsoft.com/en-us/library/dd857262.aspx. Accessed 10 May 2012.

7 Wikipedia. Active directory [online].

URL: http://en.wikipedia.org/wiki/Active_Directory. Accessed 10 May 2012.

8 Microsoft TechNet. Network location server [online].; 2 December 2010.

URL: http://technet.microsoft.com/en-us/library/gg315317.aspx. Accessed 10 May 2012.

9 Wikipedia. ISATAP [online].

URL: http://en.wikipedia.org/wiki/ISATAP. Accessed 12 May 2012.

10 Microsoft TechNet. Where to place the Forefront UAG DirectAccess server [online]. 1 February 2010.

http://technet.microsoft.com/en-us/library/ee809089.aspx#where. Accessed 10 May 2012.

11 Microsoft TechNet. Where to place the Forefront UAG DirectAccess server [online].

URL: http://technet.microsoft.com/en-us/library/ee809089.aspx#where. Accessed 10 May 2012.

12 Microsoft. Microsoft Forefront Threat Management Gateway 2010 [online].

URL: http://www.microsoft.com/TMG. Accessed 10 May 2012.

13 Microsoft TechNet. Active directory users, computers, and groups [online].

URL: http://technet.microsoft.com/en-us/library/bb727067.aspx. Accessed 10 May 2012.

14 Microsoft TechNet. Organizational units [online]. 21 January 2005.

URL: http://technet.microsoft.com/en-us/library/

cc758565%28v=ws.10%29.aspx. Accessed 10 May 2012.

15 Wikipedia. Public-key infrastructure [online].

URL: http://en.wikipedia.org/wiki/Public-key_infrastructure. Accessed 10 May 2012.

16 Wikipedia. Certificate authority [online].

URL: http://en.wikipedia.org/wiki/Certificate_authority. Accessed 10 May 2012.

17 Microsoft. IP over HTTPS (IP-HTTPS) tunneling protocol specification [online]. 30 March 2012.

URL: http://msdn.microsoft.com/en-us/library/

dd358571%28v=prot.10%29.aspx. Accessed 10 May 2012.

18 Microsoft TechNet. Using integrated NAT64 and DNS64 with Forefront UAG DirectAccess [online]. 1 February 2010.

URL: http://technet.microsoft.com/en-us/library/ee809079.aspx. Accessed 10 May 2012.

19 Shannon Fritz. UAG SP1 DirectAccess: Configuration guide [online]. 25 January 2011.

URL: http://blog.concurrency.com/infrastructure/

uag-sp1-directaccess-configuration-guide/. Accessed 10 May 2012.

20 Wikipedia. Distributed component object model [online].

URL: http://en.wikipedia.org/wiki/Distributed_Component_Object_Model. Accessed 10 May 2012.

21 Microsoft TechNet. Health registration authority [online]. 24 June 2009.

URL: http://technet.microsoft.com/en-us/library/

cc735449%28v=ws.10%29.aspx. Accessed 10 May 2012.

22 Microsoft TechNet. Network policy server [online]. 12 May 2011.

URL: http://technet.microsoft.com/en-us/network/bb629414. Accessed 10 May 2012.

23 Microsoft TechNet. Test lab guide: Demonstrate a DirectAccess multisite deployment [online]. 29 February 2012.

URL: http://technet.microsoft.com/en-us/library/hh831461.aspx. Accessed 10 May 2012.

24 Anil Erduran. Microsoft TechNet Blogs. Windows Server 2012 Direct Access – Part 1 what's new [online]. 3 May 2012.

URL: http://blogs.technet.com/b/meamcs/archive/2012/05/03/

windows-server-2012-direct-access-part-1-what-s-new.aspx. Accessed 10 May 2012.