Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Microsoft Forefront UAG – Configuring Forefront UAG as a DirectAccess Server – Part III

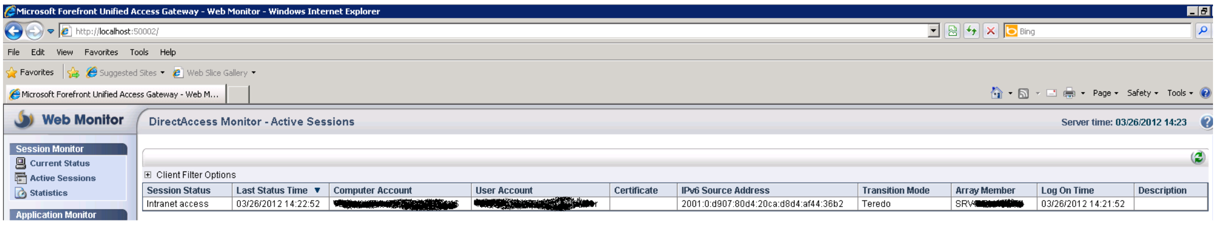
Abstract

This is a three part article series.
In part I I showed you how to configure the prerequisites for using Forefront UAG as a DirectAccess Server
In part II we talked about how to configure Forefront UAG as a DirectAccess Server
This article series will show you how to troubleshoot DirectAccess client connections and how to monitor DirectAccess clients with Forefront UAG.

Let's begin

In part I of this article series we finished installing all prerequisites for a successful Forefront UAG DirectAccess implementation. In part II we configured Forefront UAG as a DirectAccess server. This article will show you how to monitor DirectAccess clients connected to the Forefront UAG Server and how to troubleshoot DirectAccess connection problems.
After the DirectAccess group policy settings have been applied to the DirectAccess client, the client should now be able to access the corporate network with DirectAccess. It is possible to monitor the DirectAccess connection with the help of the Forefront UAG Web Monitor. Start the Forefront UAG Web Monitor and navigate to the DirectAccess Monitor and click Active Sessions. You will see all connected clients, the computer name of the DirectAccess client, the username, the type of the IPsec tunnel and the DirectAccess connection technology (Teredo, 6to4, IP-HTTPS) used.

The Forefront UAG Web Monitor allows you to monitor the connected DirectAccess clients as shown in the following screenshot:



DirectAccess Monitor - Active Sessions

Server time: 03/26/2012 14:23

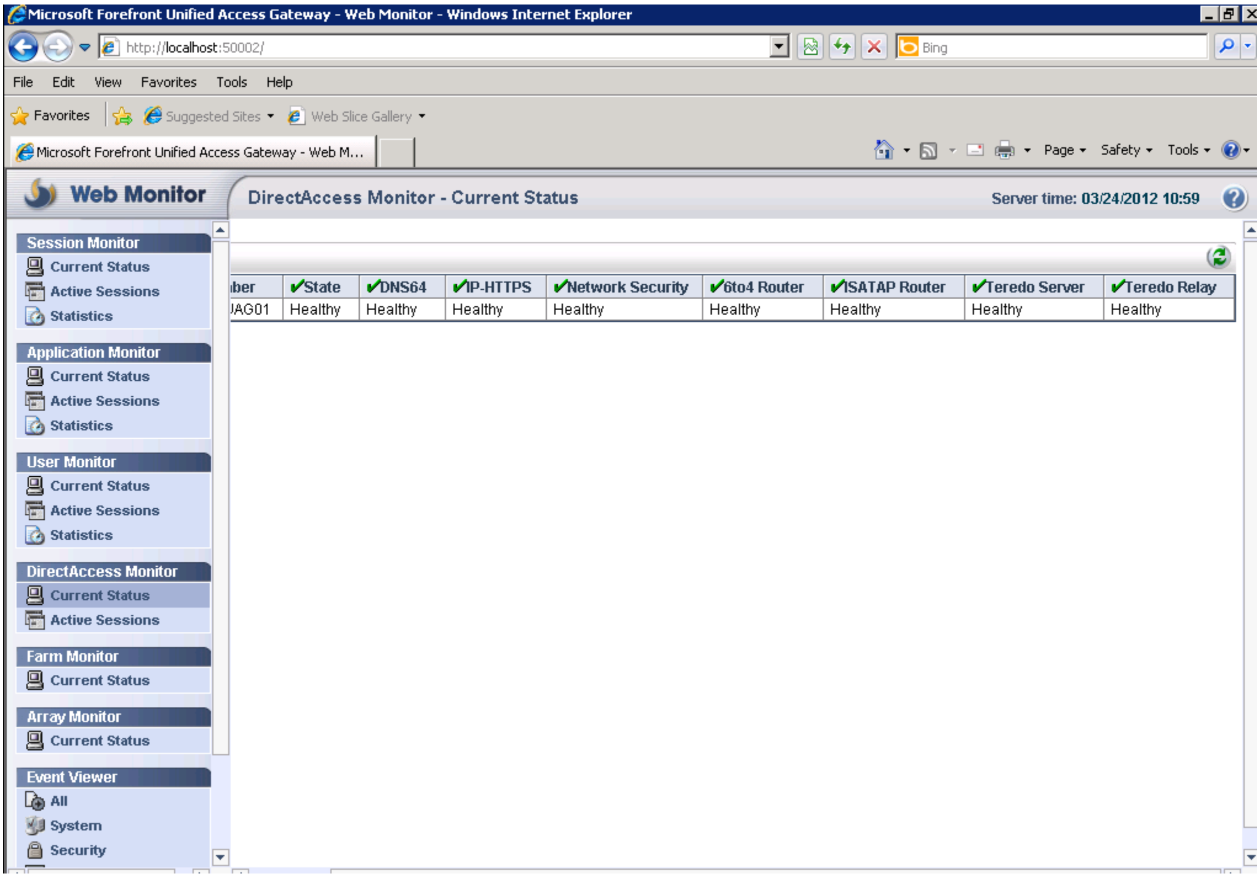
Session Status	Last Status Time ▼	Computer Account	User Account	Certificate	IPv6 Source Address	Transition Mode	Array Member	Log On Time	Description
Intranet access	03/26/2012 14:22:52	[redacted]	[redacted]		2001:0:d907:80d4:20ca:d8d4:af44:36b2	Teredo	SRV[redacted]	03/26/2012 14:21:52	

Figure 1: DirectAccess Monitor – Active sessions

It is possible to create a filter to search for example for specific client computer accounts and user accounts

Monitoring the DirectAccess status at the Forefront UAG Server

The Forefront UAG Web Monitor provides some high level information about the overall state of the health of the Forefront UAG DirectAccess implementation. Start the Forefront UAG Web Monitor and navigate to the DirectAccess Monitor and you will see the state of the Forefront UAG services in the current status view.



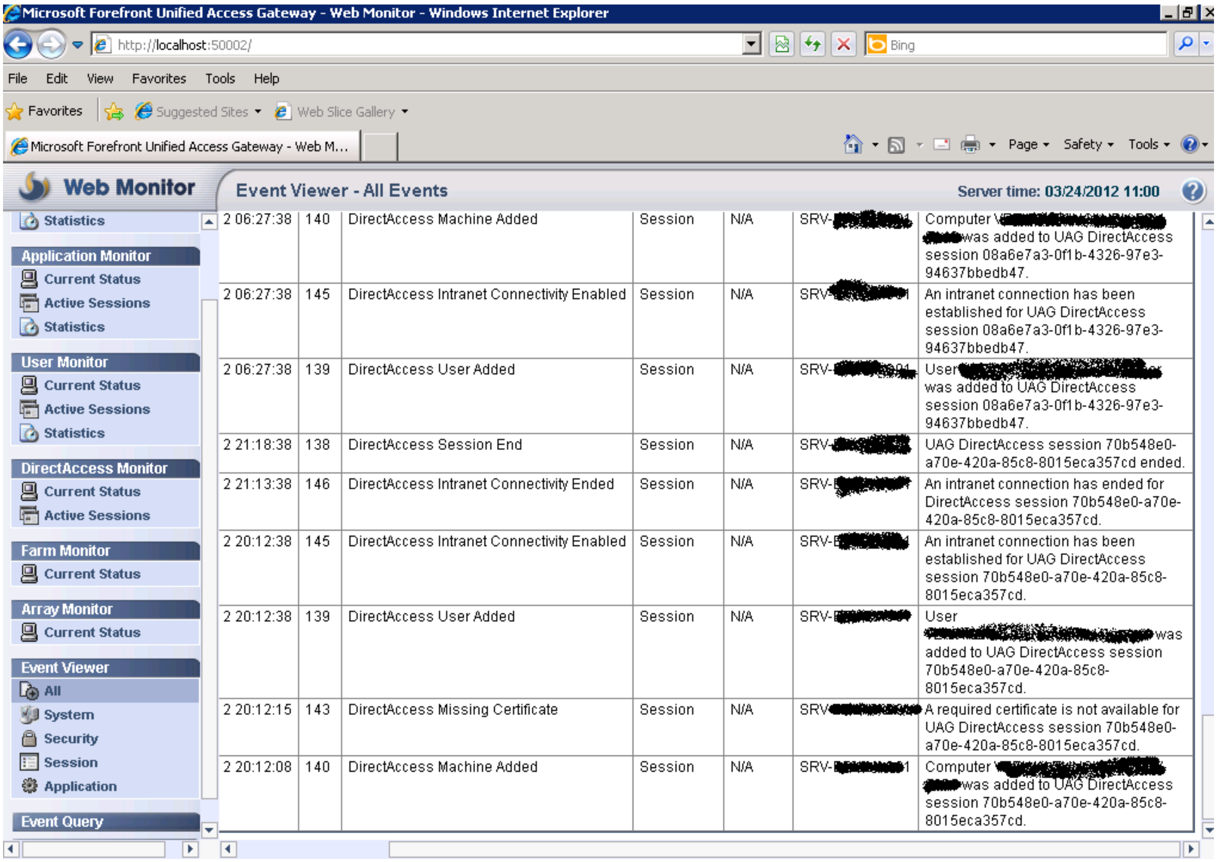
DirectAccess Monitor - Current Status

Server time: 03/24/2012 10:59

ber	✓State	✓DNS64	✓IP-HTTPS	✓Network Security	✓6to4 Router	✓ISATAP Router	✓Teredo Server	✓Teredo Relay
JAG01	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy	Healthy

Figure 2: DirectAccess Monitor – Current Status

With the Forefront UAG Web Monitor you are also able to filter the event logs created by Forefront UAG regarding DirectAccess. The following screenshot shows the event logs related to DirectAccess connections from clients.



2 06:27:38	140	DirectAccess Machine Added	Session	N/A	SRV-[redacted]	Computer [redacted] was added to UAG DirectAccess session 08a6e7a3-0f1b-4326-97e3-94637bbedb47.
2 06:27:38	145	DirectAccess Intranet Connectivity Enabled	Session	N/A	SRV[redacted]	An intranet connection has been established for UAG DirectAccess session 08a6e7a3-0f1b-4326-97e3-94637bbedb47.
2 06:27:38	139	DirectAccess User Added	Session	N/A	SRV-[redacted]	User [redacted] was added to UAG DirectAccess session 08a6e7a3-0f1b-4326-97e3-94637bbedb47.
2 21:18:38	138	DirectAccess Session End	Session	N/A	SRV-[redacted]	UAG DirectAccess session 70b548e0-a70e-420a-85c8-8015eca357cd ended.
2 21:13:38	146	DirectAccess Intranet Connectivity Ended	Session	N/A	SRV-[redacted]	An intranet connection has ended for DirectAccess session 70b548e0-a70e-420a-85c8-8015eca357cd.
2 20:12:38	145	DirectAccess Intranet Connectivity Enabled	Session	N/A	SRV-[redacted]	An intranet connection has been established for UAG DirectAccess session 70b548e0-a70e-420a-85c8-8015eca357cd.
2 20:12:38	139	DirectAccess User Added	Session	N/A	SRV-[redacted]	User [redacted] was added to UAG DirectAccess session 70b548e0-a70e-420a-85c8-8015eca357cd.
2 20:12:15	143	DirectAccess Missing Certificate	Session	N/A	SRV[redacted]	A required certificate is not available for UAG DirectAccess session 70b548e0-a70e-420a-85c8-8015eca357cd.
2 20:12:08	140	DirectAccess Machine Added	Session	N/A	SRV-[redacted]	Computer [redacted] was added to UAG DirectAccess session 70b548e0-a70e-420a-85c8-8015eca357cd.

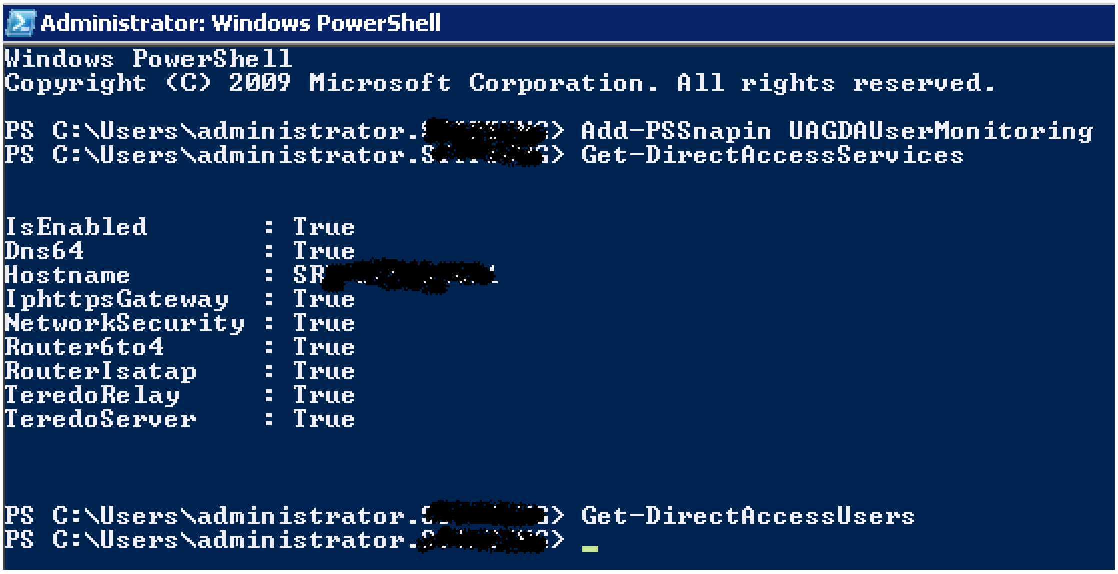
Figure 3: Forefront UAG – event viewer

Troubleshooting DirectAccess on Forefront UAG Server

Before we go deeper into troubleshooting steps on the Forefront UAG Server make sure that the DirectAccess group policy for the Forefront UAG Server has been applied to the system.

Next, check if all Forefront UAG services are running. Specially keep attention for the Microsoft Forefront UAG DNS64 Service which is responsible for DNS IPv4 to IPv6 translation.

Forefront UAG comes with a Powershell SnapIn for UAG DirectAccess monitoring which monitors the current Forefront UAG DirectAccess users and the status of Forefront UAG services, as shown in the following screenshot.



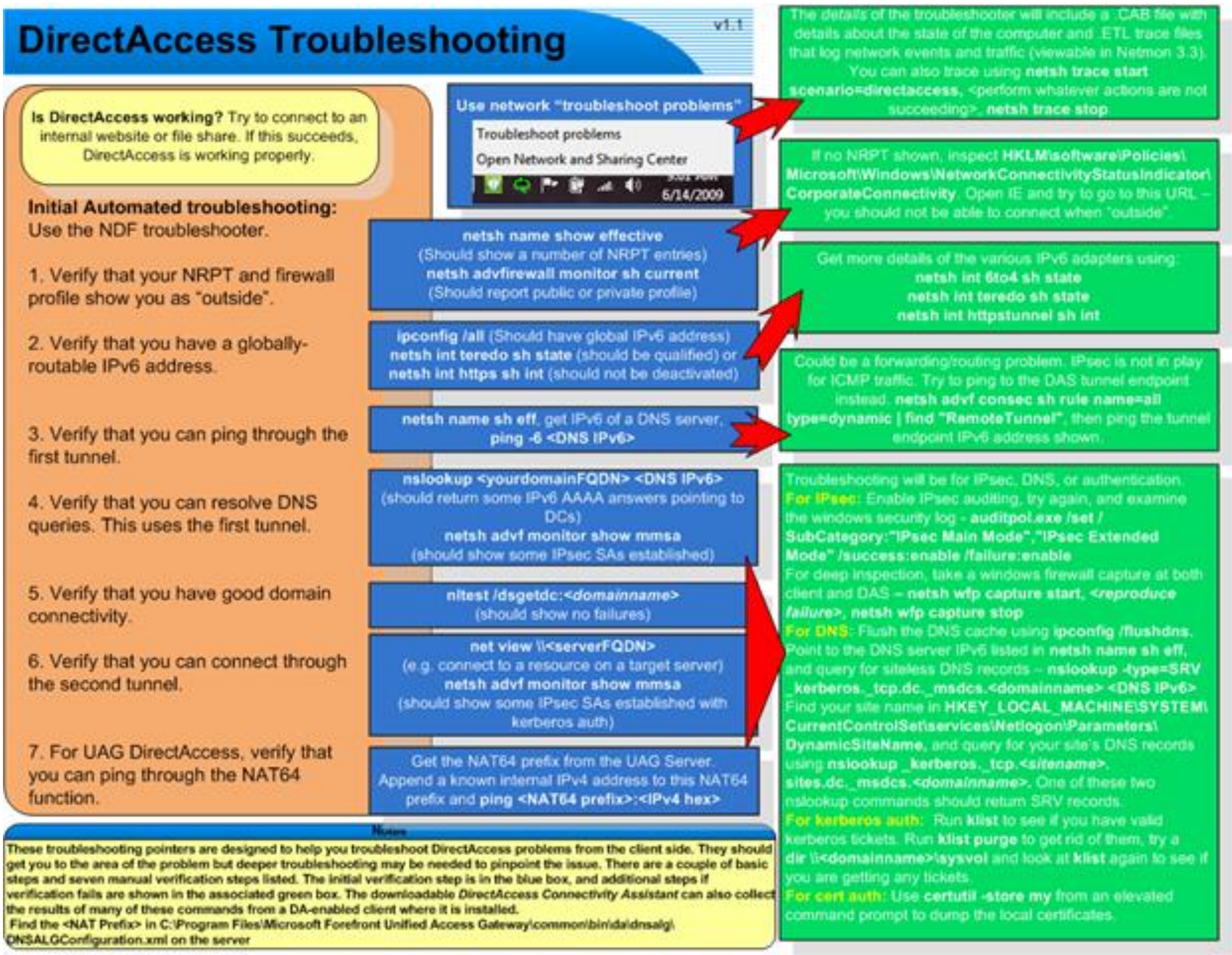
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.[redacted]> Add-PSSnapin UAGDAUserMonitoring
PS C:\Users\administrator.[redacted]> Get-DirectAccessServices


IsEnabled         : True
Dns64             : True
Hostname          : [redacted]
IphttpsGateway    : True
NetworkSecurity   : True
Router6to4        : True
RouterIsatap      : True
TeredoRelay       : True
TeredoServer      : True



PS C:\Users\administrator.[redacted]> Get-DirectAccessUsers
PS C:\Users\administrator.[redacted]> _
```

Figure 4: Forefront UAG PowerShell Snap In

Fore more DirectAccess related troubleshooting steps I recommend to read the following article.

Common DirectAccess troubleshooting

For common DirectAccess troubleshooting guidelines Microsoft provides a great flowchart for troubleshooting:



DirectAccess Troubleshooting

v1.1

Is DirectAccess working? Try to connect to an internal website or file share. If this succeeds, DirectAccess is working properly.

Initial Automated troubleshooting: Use the NDF troubleshooter.

Use network "troubleshoot problems"

The details of the troubleshooter will include a .CAB file with details about the state of the computer and .ETL trace files that log network events and traffic (viewable in Netmon 3.3). You can also trace using **netsh trace start scenario=directaccess**, <perform whatever actions are not succeeding>, **netsh trace stop**

1. Verify that your NRPT and firewall profile show you as "outside".

netsh name show effective (Should show a number of NRPT entries) **netsh advfirewall monitor sh current** (Should report public or private profile)

If no NRPT shown, inspect **HKLM\software\Policies\Microsoft\Windows\NetworkConnectivityStatusIndicator\CorporateConnectivity**. Open IE and try to go to this URL – you should not be able to connect when "outside".

2. Verify that you have a globally-routable IPv6 address.

ipconfig /all (Should have global IPv6 address) **netsh int teredo sh state** (should be qualified) or **netsh int https sh int** (should not be deactivated)

Get more details of the various IPv6 adapters using: **netsh int 6to4 sh state** **netsh int teredo sh state** **netsh int httpstunnel sh int**

3. Verify that you can ping through the first tunnel.

netsh name sh eff, get IPv6 of a DNS server, **ping -6 <DNS IPv6>**

Could be a forwarding/routing problem. IPsec is not in play for ICMP traffic. Try to ping to the DAS tunnel endpoint instead. **netsh advf consec sh rule name=all type=dynamic | find "RemoteTunnel"**, then ping the tunnel endpoint IPv6 address shown.

4. Verify that you can resolve DNS queries. This uses the first tunnel.

nslookup <yourdomainFQDN> <DNS IPv6> (should return some IPv6 AAAA answers pointing to DCs) **netsh advf monitor show mmsa** (should show some IPsec SAs established)

5. Verify that you have good domain connectivity.

nltest /dsgetdc:<*domainname*> (should show no failures)

6. Verify that you can connect through the second tunnel.

net view \\<serverFQDN> (e.g. connect to a resource on a target server) **netsh advf monitor show mmsa** (should show some IPsec SAs established with kerberos auth)

Troubleshooting will be for IPsec, DNS, or authentication. For IPsec: Enable IPsec auditing, try again, and examine the windows security log - **auditpol.exe /set / SubCategory:"IPsec Main Mode","IPsec Extended Mode" /success:enable /failure:enable** For deep inspection, take a windows firewall capture at both client and DAS – **netsh wfp capture start, <*reproduce failure*>, netsh wfp capture stop**

For DNS: Flush the DNS cache using **ipconfig /flushdns.** Point to the DNS server IPv6 listed in **netsh name sh eff**, and query for siteless DNS records – **nslookup -type=SRV _kerberos._tcp.dc._msdcs.<domainname> <DNS IPv6>** Find your site name in **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Netlogon\Parameters\DynamicSiteName**, and query for your site's DNS records using **nslookup _kerberos._tcp.<*sitename*>.sites.dc._msdcs.<*domainname*>.** One of these two nslookup commands should return SRV records.

For kerberos auth: Run **klist** to see if you have valid kerberos tickets. Run **klist purge** to get rid of them, try a **dir \\<domainname>\sysvol** and look at **klist** again to see if you are getting any tickets.

For cert auth: Use **certutil -store my** from an elevated command prompt to dump the local certificates.

7. For UAG DirectAccess, verify that you can ping through the NAT64 function.

Get the NAT64 prefix from the UAG Server. Append a known internal IPv4 address to this NAT64 prefix and **ping <NAT64 prefix>:<IPv4 hex>**

Notes

These troubleshooting pointers are designed to help you troubleshoot DirectAccess problems from the client side. They should get you to the area of the problem but deeper troubleshooting may be needed to pinpoint the issue. There are a couple of basic steps and seven manual verification steps listed. The initial verification step is in the blue box, and additional steps if verification fails are shown in the associated green box. The downloadable *DirectAccess Connectivity Assistant* can also collect the results of many of these commands from a DA-enabled client where it is installed.
Find the <NAT Prefix> in C:\Program Files\Microsoft Forefront Unified Access Gateway\common\bin\da\dnsalg\DNSALGConfiguration.xml on the server

Figure 5: DirectAcess troubleshooting reference (Source: http://blogs.technet.com/b/edgeaccessblog/archive/2010/04/07/basic-troubleshooting-steps-for-uag-directaccess.aspx)

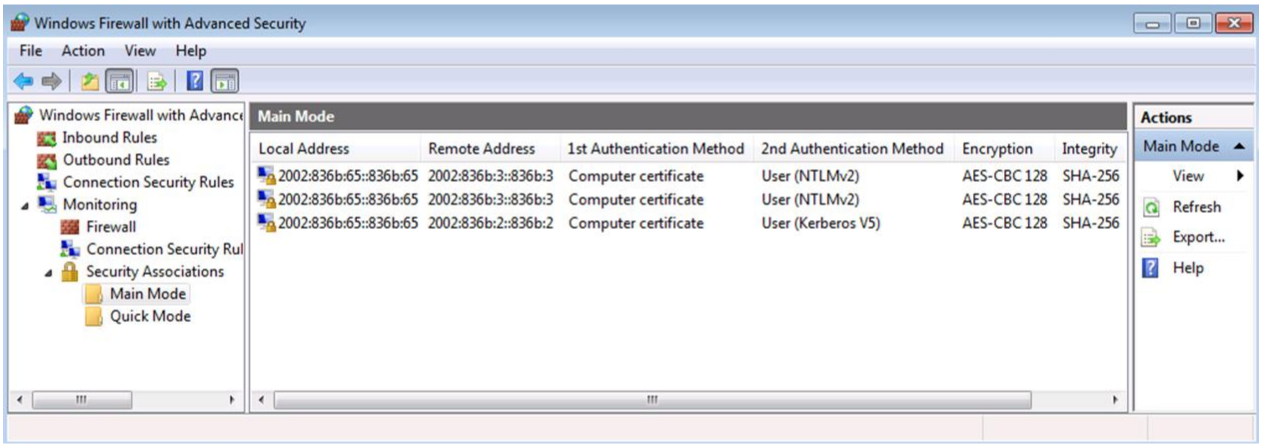
Troubleshooting the DirectAccess client computer

Before we go deeper into troubleshooting makes sure that the following requirements are fulfilled:

- Windows 7 Ultimate or Enterprise
- DirestAccess client must be joined to the Active Directory Domain
- Computer certificate stored in the local computer certificate store
- DirectAccess group policy has been applied
- DirectAccess client must have a global IPv6 address
- Check NRPT (Name Resolution Policy Table) on the DirectAccess client computer
- Ensure that the Windows Firewall on the DirectAccess client is activated and the public Firewall profile is used

Windows Firewall

As a next step check, if the Windows Firewall on the DirectAccess client computer has been enabled, the public Windows Firewall profile is used and the DirectAccess group policy settings has been applied to the client as shown in the following screenshot.



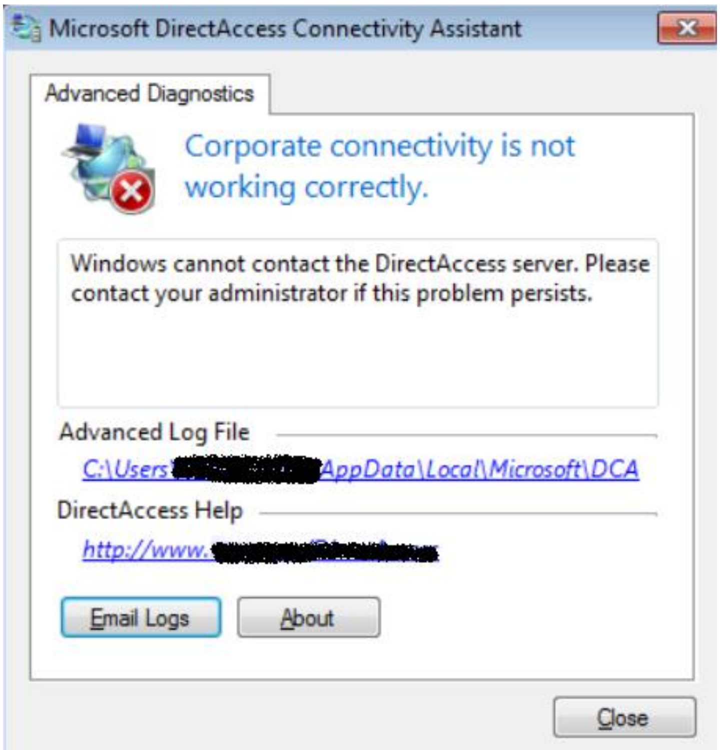
Main Mode

Local Address	Remote Address	1st Authentication Method	2nd Authentication Method	Encryption	Integrity
2002:836b:65::836b:65	2002:836b:3::836b:3	Computer certificate	User (NTLMv2)	AES-CBC 128	SHA-256
2002:836b:65::836b:65	2002:836b:3::836b:3	Computer certificate	User (NTLMv2)	AES-CBC 128	SHA-256
2002:836b:65::836b:65	2002:836b:2::836b:2	Computer certificate	User (Kerberos V5)	AES-CBC 128	SHA-256

Figure 6: Windows Firewall with Advanced Security on the DirectAccess client

DCA (DirectAccess Connectivity Assistant)

As an optional step it is possible to automatically deploy the DCA software on the DirectAccess computer. The DCA will tell the end user if he has successfully established a connection to the corporate network and if there are some connection problems the DCA displays a warning message that DirectAccess connectivity cannot be established. The end user is now able to generate a set of log files regarding DirectAccess which may be helpful for Forefront UAG Administrators to analyse the reason for the connectivity problem.



Corporate connectivity is not working correctly.

Windows cannot contact the DirectAccess server. Please contact your administrator if this problem persists.

Advanced Log File

C:\Users\[redacted]AppData\Local\Microsoft\DCA

DirectAccess Help

http://www.[redacted]

Figure 7: DCA and Advanced Log File creation

Helpful NETSH commands for troubleshooting

Troubleshooting DirectAccess at client and Server side is based on a number of command line tools like Netsh. Here are some helpful Netsh commands at DirectAccess client side:

netsh dns show state

Displays the DirectAccess status and general configuration state.

netsh namespace show policy

This command displays the content of the NRPT (Name Resolution Policy Table) at client side, created by the group policy wizard in Forefront UAG.

netsh namespace show effectivepolicy

This command shows the active NRPT content on the client and not only the group policy settings.

The following two commands show the state of the Teredo and IP-HTTPS interface:

```
netsh interface teredo show state
netsh interface httpstunnel show interfaces
```

The following three commands are very helpful to see the state of the Windows Firewall on the DirectAccess client, the current Firewall profile used and the created IPSec Main mode Security Association (SA)

```
netsh advfirewall monitor show firewall
netsh advfirewall show currentprofile
netsh advfirewall monitor show mmsa
```

Conclusion

In this third article I showed you how to monitor DirectAccess client connections and how to troubleshoot DirectAccess connectivity problems. In my opinion troubleshooting DirectAccess connectivity problems can be painful but with the right tools and techniques you should be able to successfully resolve the cause of DirectAccess connection problems.

Related links

DirectAccess Troubleshooting Guide
http://technet.microsoft.com/en-us/library/ee624056(v=ws.10).aspx
Test Lab Guide: Troubleshoot DirectAccess
http://www.microsoft.com/download/en/details.aspx?id=22210
General Methodology for Troubleshooting DirectAccess Connections
http://technet.microsoft.com/en-us/library/ee624058(v=ws.10).aspx
New UAG DirectAccess Troubleshooting Content on the TechNet Wiki
http://blogs.technet.com/b/tomshinder/archive/2010/12/14/new-uag-directaccess-troubleshooting-content-on-the-technet-wiki.aspx
Microsoft Forefront UAG – Overview of Microsoft Forefront UAG
http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html
Forefront UAG technical overview
http://technet.microsoft.com/en-us/library/ee690443.aspx