

Forefront UAG mit DirectAccess

Implementierungsumgebung:

- Windows Server 2008 R2 englisch mit zwei Netzwerkkarten als Forefront UAG Server parallel zu der TMG Enterprise Umgebung als Firewall. Der Forefront UAG Server steht in der DMZ vor einer nicht Microsoft Firewall ☹
- Windows 7 Ultimate oder Enterprise Client fuer DirectAccess Zugriff
- Windows Server 2008 R2 Enterprise CA
- Windows Server 2008 R2 Enterprise als NLS Server

Weitere Informationen:

<http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html>

<http://www.it-training-grote.de/download/Forefront-UAG.pdf>

<http://blogs.technet.com/b/tomshinder/archive/2010/08/03/how-to-configure-uag-to-publish-your-private-certificate-revocation-list.aspx>

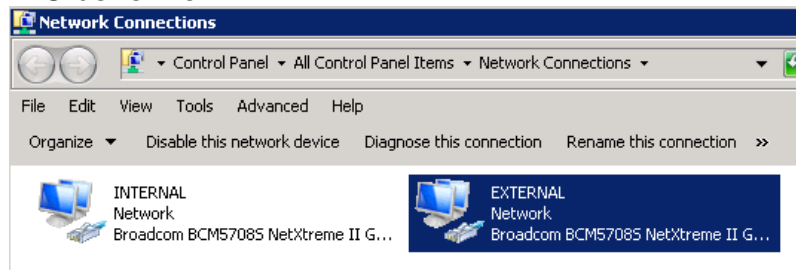
<http://technikblog.rachfahl.de/wp-content/uploads/2010/07/Direct-Access-Howto.pdf>

<http://technet.microsoft.com/en-us/library/ee861167.aspx>

<http://www.microsoft.com/downloads/details.aspx?FamilyID=9A87EFE8-E254-4473-8A26-678ADEA6D9E9&displaylang=en>

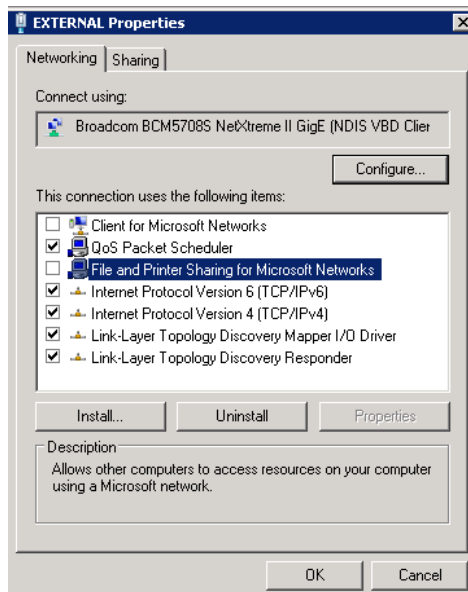
Auf dem Forefront UAG Server

NIC benennen

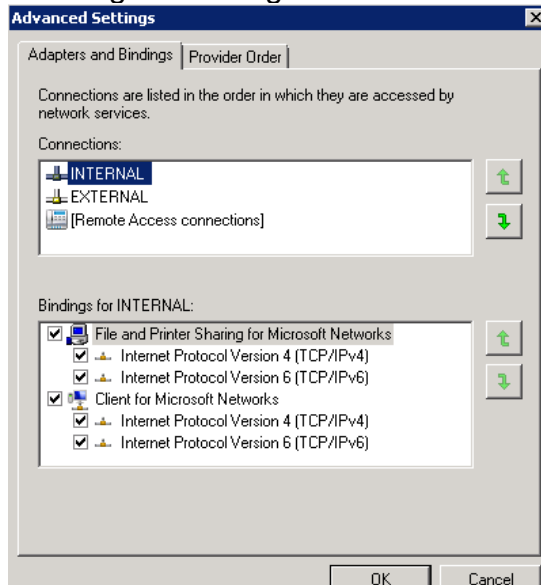


Netzwerkkarte Extern

NetBT kann am externen Interface deaktiviert werden!



Bindungsreihenfolge – INTERNAL muss oben stehen



DNS Server GlobalqueryBlocklist ISATAP

Die GlobalQueryBlocklist muss von JEDEM DNS Server im LAN fuer ISATAP entfernt werden.

```
Administrator: Eingabeaufforderung

C:\>dnscmd srv-walk.00000000 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000002 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000003 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000004 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000005 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000006 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000007 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000008 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.

C:\>dnscmd srv-walk.00000009 /config /globalqueryblocklist wpad
Registrierungseigenschaft globalqueryblocklist wurde zurückgesetzt.
Der Befehl wurde erfolgreich ausgeführt.
```

ISATAP Eintrag erstellen fuer interne IP des UAG Server

A Record ISATAP = 10.80.20.29

Neuer Host

Name (bei Nichtangabe wird übergeordneter Domänenname verwendet):
ISATAP

Vollqualifizierter Domänenname:
ISATAP.local.

IP-Adresse:
10.80.20.29

☒ Verknüpfen PTR-Eintrag erstellen

☐ Authentifizierte Benutzer können DNS-Einträge mit demselben Besitzernamen aktualisieren

Host hinzufügen

Abbrechen

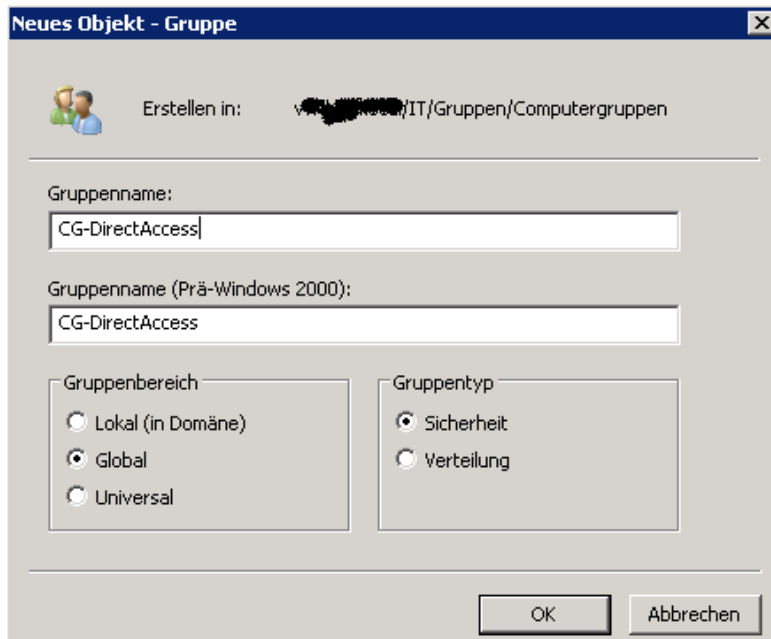
Windows Firewallausnahmen fuer ICMPv6

GPO erstellen fuer DC und NLS Server

Anmerkung: Auf den Server kann die Firewall auch ausgeschaltet sein, auf den DirectAccess Clients muss diese eingeschaltet sein, wegen der vom DirectAccess Wizard erstellten Verbindungsrichtlinien!

Globale Windows Gruppe fuer DirectAccess Clients

Name = CG-DirectAccess



Windows 7 Client (Ultimate oder Enterprise) Maschinen in die Gruppe aufnehmen

Modifizierung des CRL Verteilungspfad (CDP)

Es wird eine Windows Server 2008 R2 Enterprise CA verwendet

Name = SRV-XXX-PKI01.XXX.LOCAL

Fuer das Publishing der CRL ueber das separate TMG Array wird ein oeffentlicher Hostname benoetigt:

Name = Legacy.xxxx.de → 217.x.xxx.214

Damit von der CA ausgestellte Zertifikate den CRL Distribution Point auf HTTP mit dem externen Namen gesetzt bekommen, muss die CA gepatched werden. Das geht mit CERTUTIL Befehlen und/oder diesem netten Script, was mir freundlicherweise Carsten Zuege zur Verfuegung gestellt hat – Danke Carsten!. Der http-Pfad muss ersetzt werden durch den oeffentlichen DNS-Namen. Der CRL Pfad wird spaeter von Forefront TMG veroeffentlicht. Angepasst werden muss der CN fuer die AD Konfigurationspartition und der http CRL Pfad.

```

CA-PAST-Config - Editor
Datei Bearbeiten Format Ansicht ?

::Declare Configuration NamingContext
certutil -setreg CA\DSConfigDN CN=Configuration,DC=B,DC=
::Define CRL Publication Intervals
certutil -setreg CA\CRLPeriodUnits 1
certutil -setreg CA\CRLPeriod "weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 1
certutil -setreg CA\CRLDeltaPeriod "days"
::Apply the required CDP Extension URLs
PAUSE
certutil -setreg CA\CRLPublicationURLs "65:%windir%\system32\CertSrv\CertEnroll\%3%8%9.cr1\n79:ldap:///CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10\n6: http://10.10.10.10/certenroll/%3%8%9.cr1"
PAUSE
::Apply the required AIA Extension URLs
certutil -setreg CA\CACertPublicationURLs "1:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.crt\n3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11\n2: http://10.10.10.10/certenroll/%1_%3%4.crt"
PAUSE
::Enable all auditing events for the Enterprise Root-CA
certutil -setreg CA\AuditFilter 127
PAUSE
::Set Validity Period for Issued Certificates
certutil -setreg CA\ValidityPeriodUnits 5
certutil -setreg CA\ValidityPeriod "Years"
PAUSE
::Restart Certificate Services
net stop certsrv & net start certsrv

```

Anmerkung: Publish ueber Forefront UAG geht auch:

<http://blogs.technet.com/b/tomshinder/archive/2010/08/03/how-to-configure-uag-to-publish-your-private-certificate-revocation-list.aspx>

Nach Aenderung

Eigenschaften von RootCA

Speicherung | Zertifikatverwaltungen | Registrierungs-Agents
 Überwachung | Wiederherstellungs-Agents | Sicherheit
 Allgemein | Richtlinienmodul | Beendigungsmodul | Erweiterungen

Erweiterung auswählen:
 Sperlisten-Verteilungspunkt

Geben Sie Standorte an, von denen Benutzer eine Zertifikatsperlliste erhalten können.

C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix>\I
 ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNa
 http://10.10.10.10/certenroll/<CaName><CRLNameSuffix>

Hinzufügen... Entfernen

☐ Sperlisten an diesem Ort veröffentlichen

☐ In alle Sperlisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll

☐ In Sperlisten einbeziehen. Wird z. Suche von Deltasperlisten verwendet

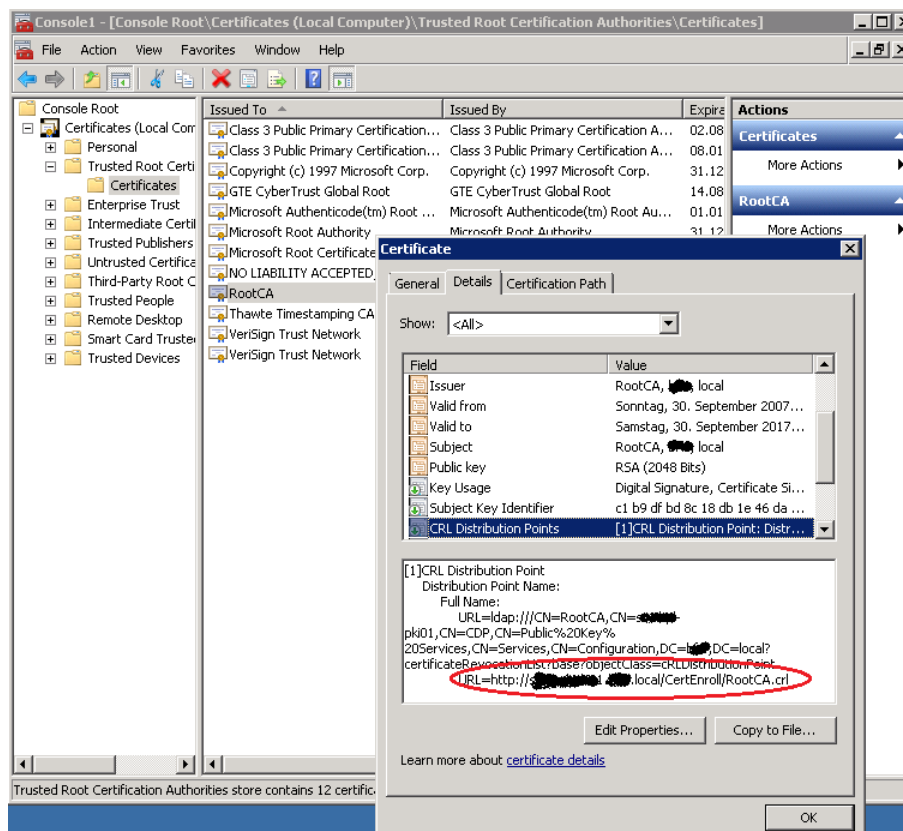
☐ In CDP-Erweiterung des ausgestellten Zertifikats einbeziehen

☐ Deltasperlisten an diesem Ort veröffentlichen

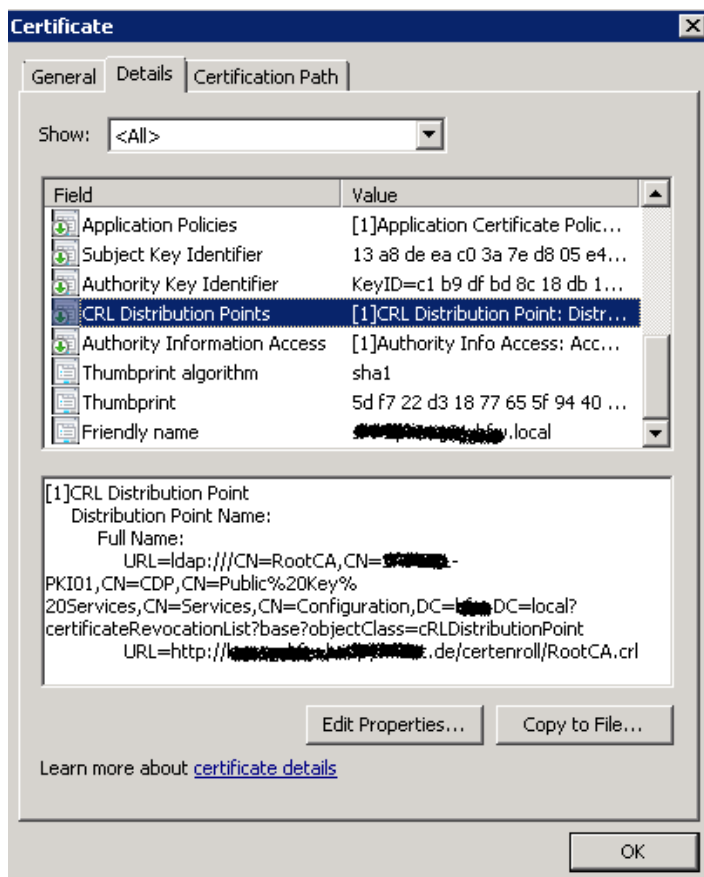
☐ In die IDP-Erweiterung ausgestellter CRLs einbeziehen

OK Abbrechen Übernehmen Hilfe

CRL Pfad vor Modifizierung – Zu sehen in den Zertifikateigenschaften



CRL Pfad in einem neu ausgestellten Zertifikat



CRL ueber Forefront TMG veroeffentlichen

1 CA-CRL Zulassen HTTP CA-CRL SRV-...PKIO... Alle Benutzer

Parameter

Webserververoeffentlichung

Kein HTTPS

Pfad /certenroll/*

Keine Authentifizierung

Keine Authentifizierungsdelegation

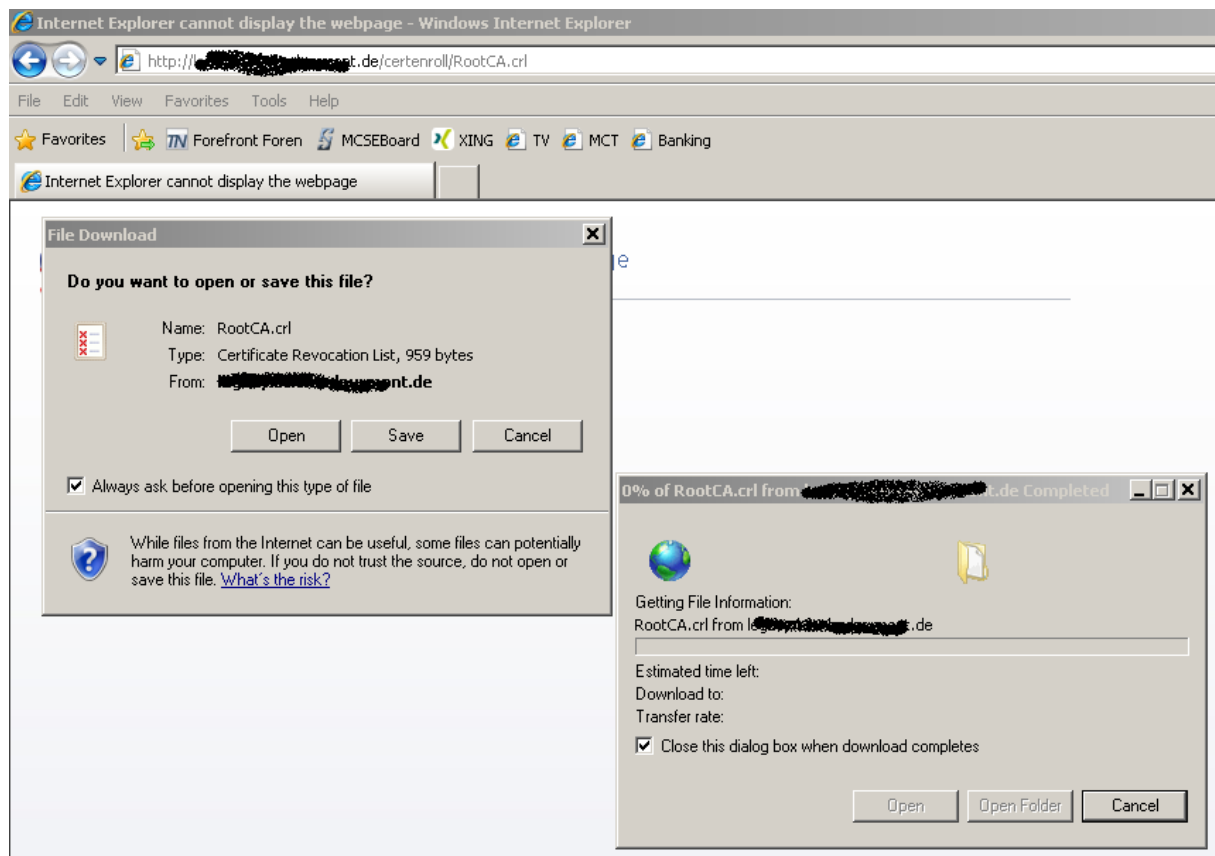
Keine HTTP Komprimierung

Alle Benutzer

Zeitplan = Immer

Oeffentlicher Name der Name, welche als CDP in den CA Eigenschaften steht

Ueberpruefen



Testen der CRL

certutil -URL http://crl.domain.de/crld/ca.crl

URL Retrieval Tool

Status	Type	Url
--------	------	-----

Timeout (sec) ☐ Sign LDAP Traffic

Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

Retrieve

☐ Certs (from AIA)
☒ CRLs (from CDP)
☐ OCSP (from AIA)

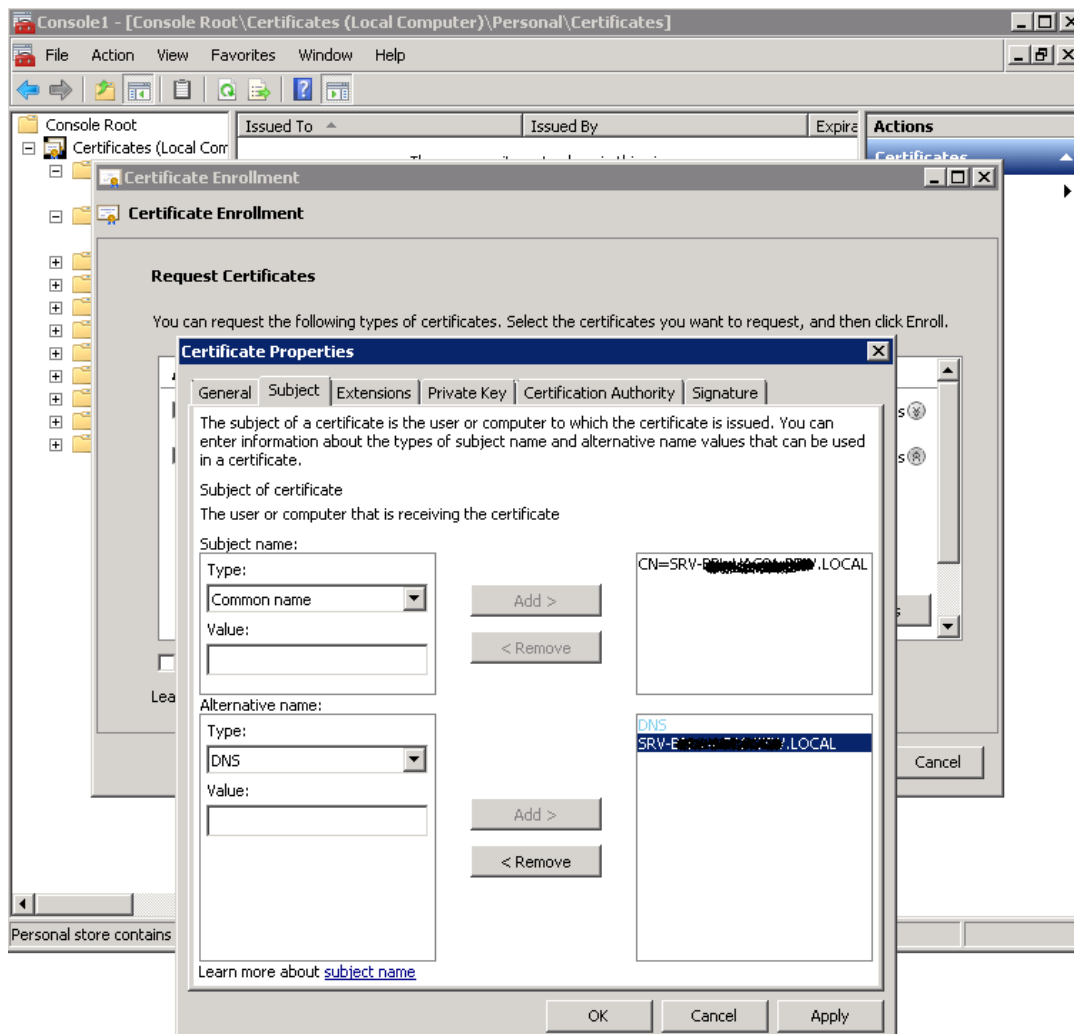
Url to Download

Computerzertifikat fuer UAG Server

Interner DNS FQDN – SAN ist meines Erachtens nicht noetig. Steht aber so im UAG Step by Step Guide von MS!

CN = SRV-xxx-xxx.xxx.LOCAL

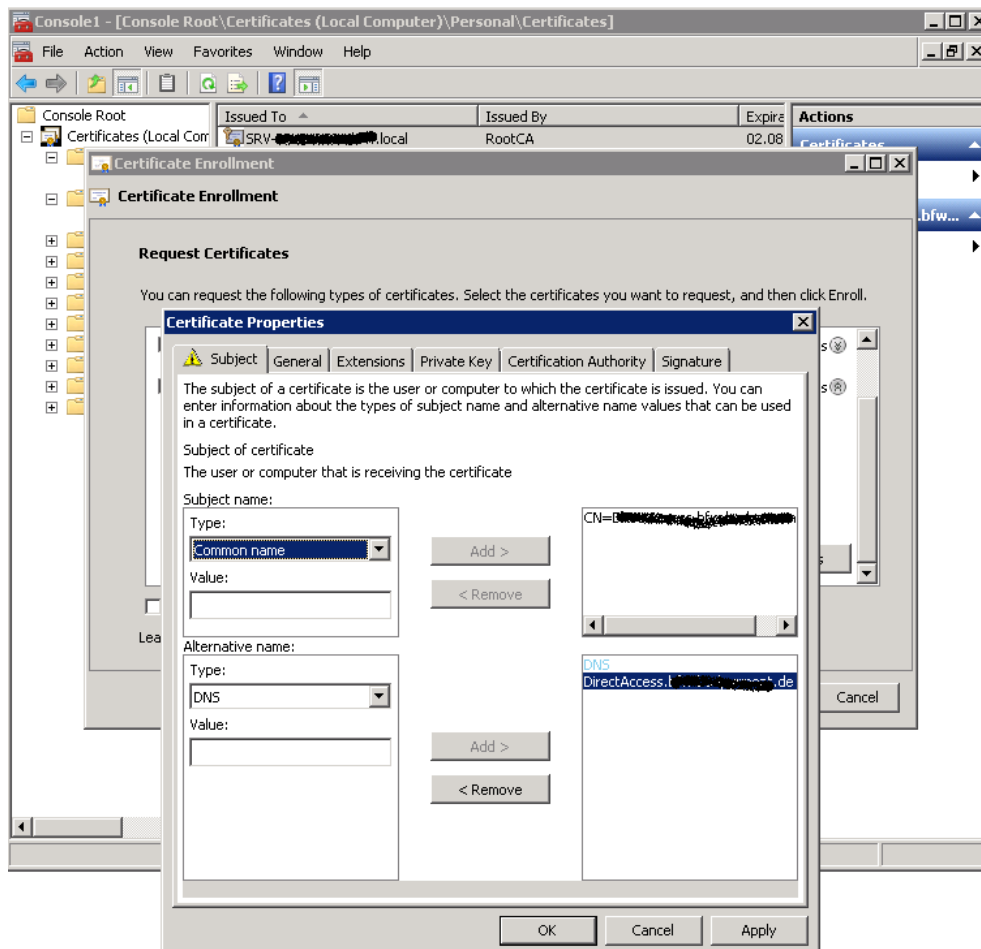
SAN = SRV-xxx-xxx.xxx.LOCAL



Webserverzertifikat fuer UAG Server

CN = DirectAccess.xxx.de → A Record auf erste oeffentliche IP, welche auf dem externen Interface des Forefront UAG Server gebunden ist!
 SAN = DirectAccess.xxx.de

WICHTIG: Der CN, welcher hier verwendet wird, muss im Public DNS auf die erste oeffentliche IP gebunden sein, welche am externen Interface des Microsoft Forefront UAG Server verwendet wird.



2 Public IPv4 Adressen auf dem externen Interface von Forefront UAG

217.x.xxx.212 → DirectAccess.xxx.de
217.x.xxx.213

ACHTUNG: [http://technet.microsoft.com/en-us/library/ee844123\(Ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee844123(Ws.10).aspx)

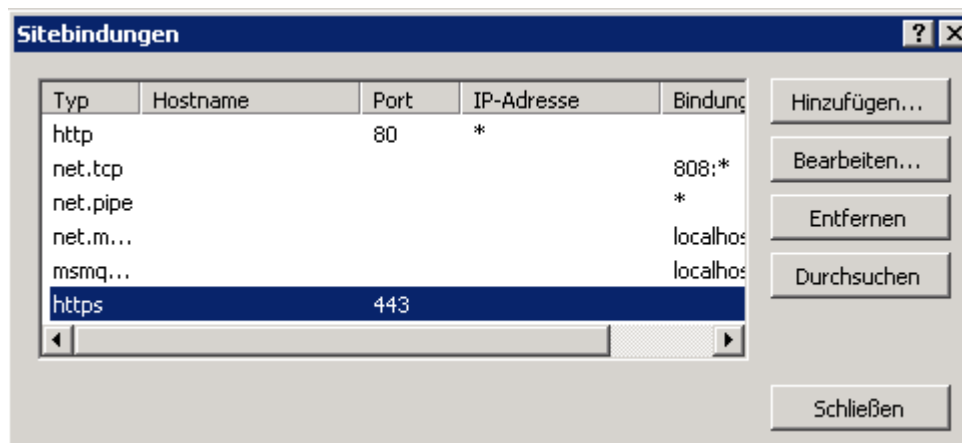
NLS Server konfigurieren

Anhand des NLS Servers prüft der DirectAccess Client, ob er im LAN oder im Internet steht. Der NLS Server muss ein Webserver (IIS; Apache etc.) sein, auf dem eine HTTPS-Bindung existiert und das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt ist, welcher der DirectAccess Client und der Forefront UAG Server vertrauen.

xx.xx.xxx.LOCAL

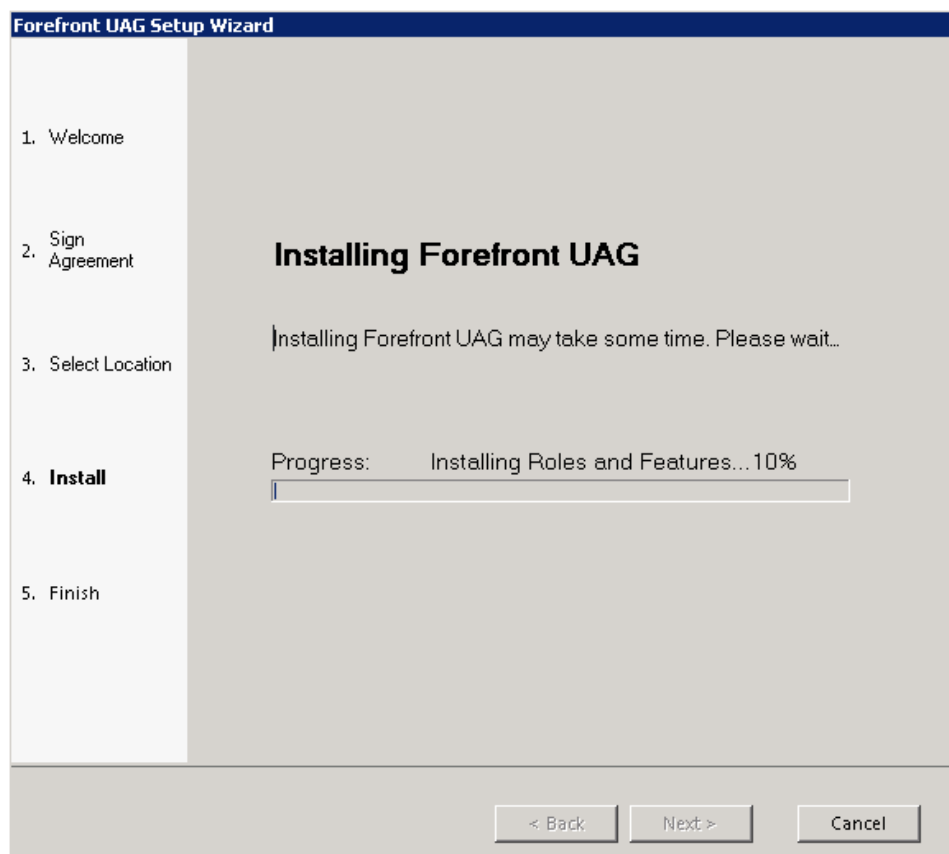
Der NLS sollte hochverfügbar gemacht werden, weil der DA Client anhand der Verfügbarkeit des NLS prüft, ob er im LAN oder im Internet steht.

Achtung: Der NLS wird von der NRPT ausgeschlossen und ist somit vom DirectAccess Client, wenn dieser nicht mit dem LAN verbunden ist, nicht erreichbar. Es muss also ein NLS verwendet werden, der nur im LAN erreichbar sein muss.

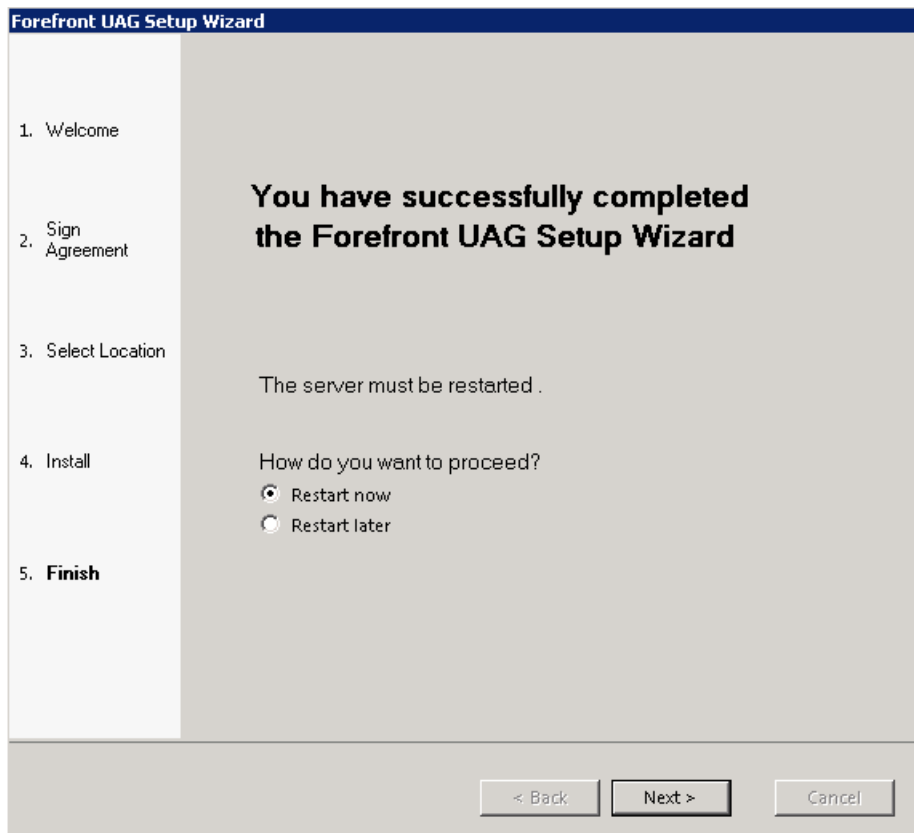


Forefront UAG Installation und Konfiguration

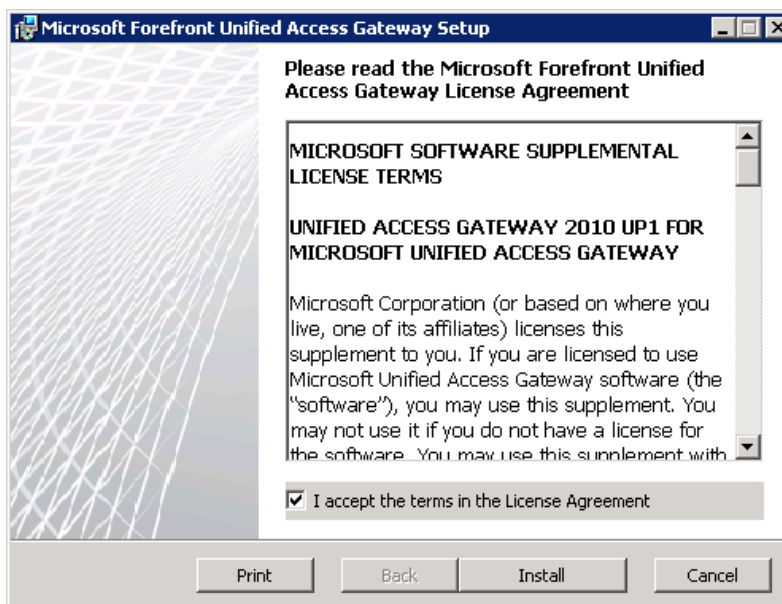
Die Installation erfolgt auf einem voll gepatchten Windows Server 2008 R2 mit zwei Netzwerkkarten.



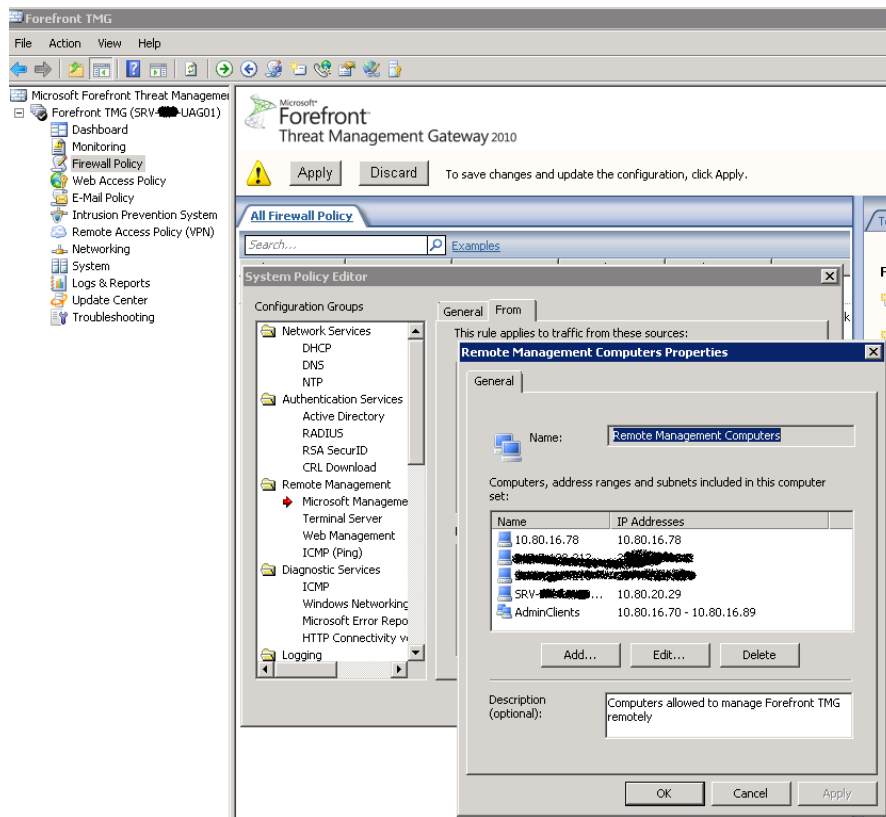
Server rebooten



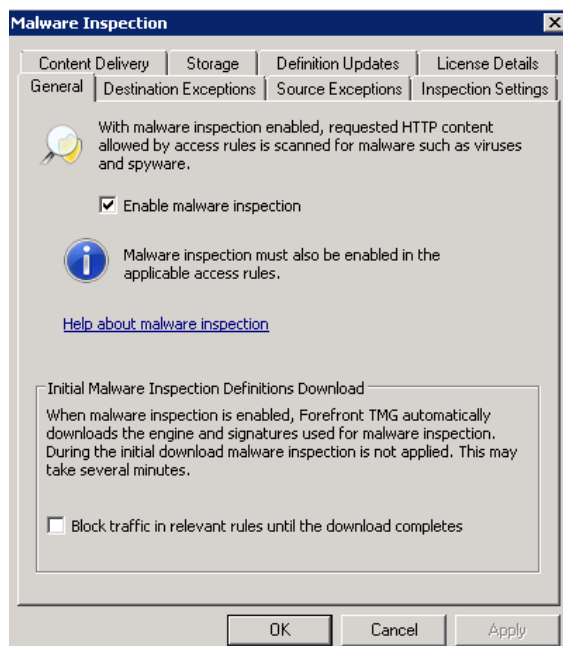
Forefront UAG Update 1 installieren



Systemrichtlinie konfigurieren fuer Remote Computer Zugriff

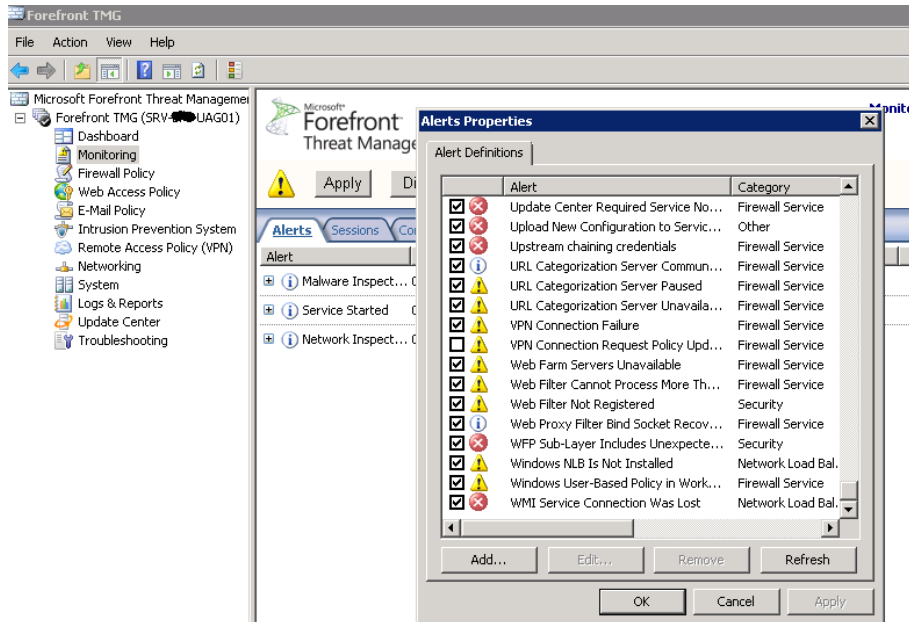


Malware Inspection ausschalten

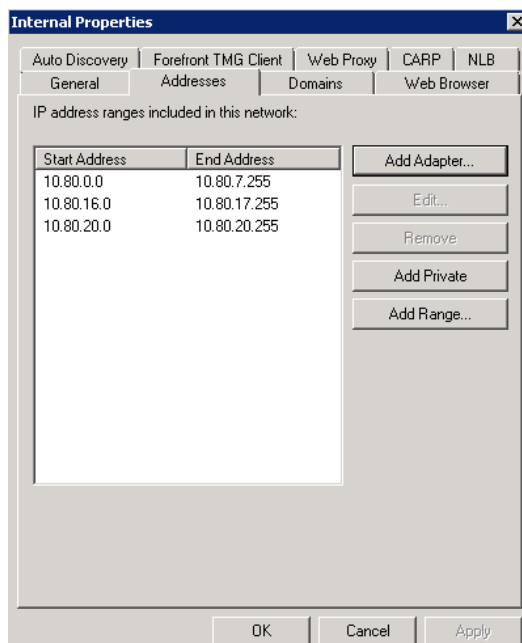


Logging/Alerting konfigurieren

WFP Filter Alerting Konflikt ausschalten



Interne Netzwerke am TMG des UAG eintragen, da der UAG nur Proxy in der DMZ ist und die Netze hinter dem UAG ueber ein Forefront TMG Enterprise Array erreichen muss.



Statische Routen konfigurieren

Microsoft Forefront Threat Management Gateway 2010

Network Enterprise

Networks Network Sets Network Rules Network Adapters **Routing** Web Chaining ISP Redundancy

Tasks Help

Network Destination	Netmask	Gateway/Interf...	Metric
Network Topology Routes			
10.80.0.0	255.255.248.0	10.80.20.1	0
10.80.16.0	255.255.254.0	10.80.20.1	0

Routing Tasks

- Create Network Topology Route
- Refresh Now

UAG Getting Started Assistent

Network Configuration Wizard

Define Network Adapters

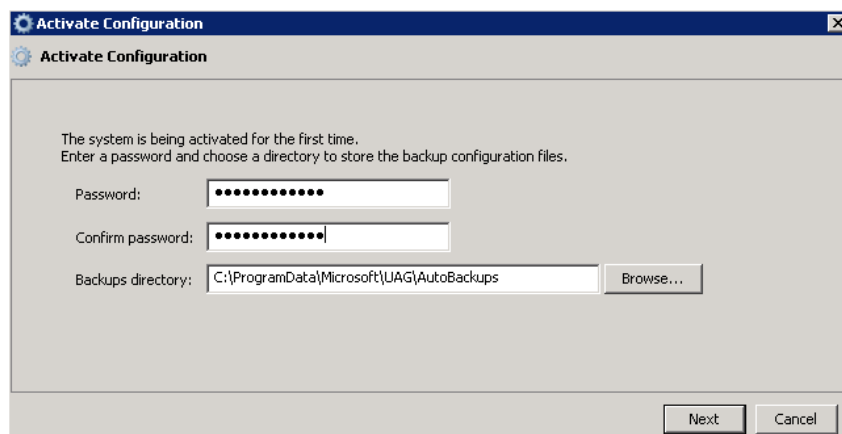
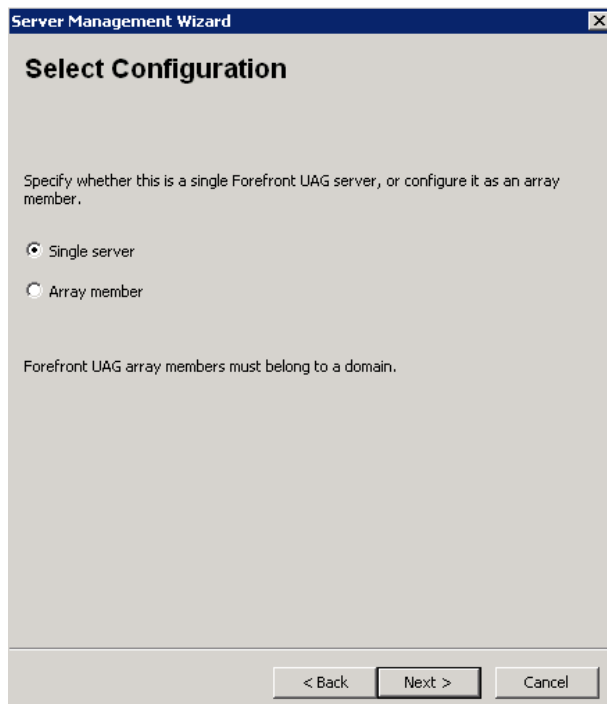
Specify how network adapters are connected to your network, and modify the network adapter settings.

Adapter name	Internal	External	Unassigned
EXTERNAL		✓	
INTERNAL	✓		
SSL Network Tunneling			✓

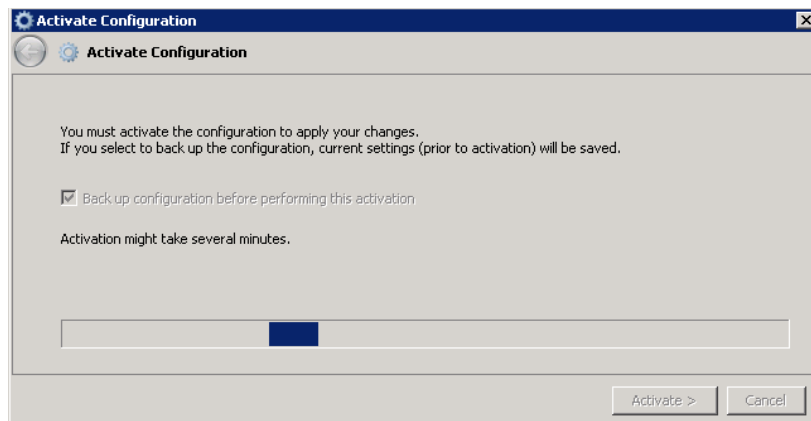
Adapter properties:

Adapter name: INTERNAL
IP DHCP enabled: No
IP address: 10.80.20.29
Subnet mask: 255.255.255.0
Default gateway: 10.80.20.1
DNS DHCP enabled: No
DNS server(s): 10.80.20.2,10.80.20.3
Static route: No

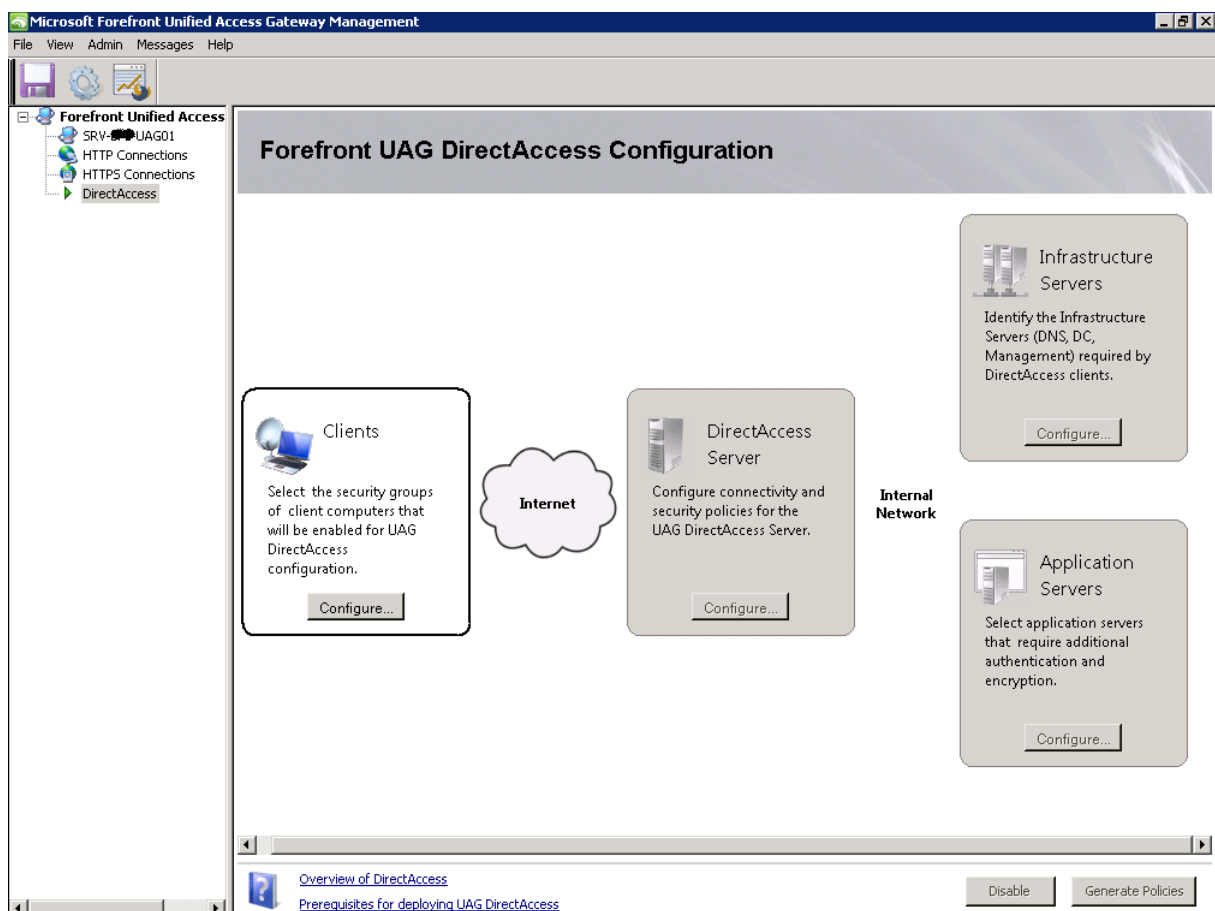
< Back Next > Cancel



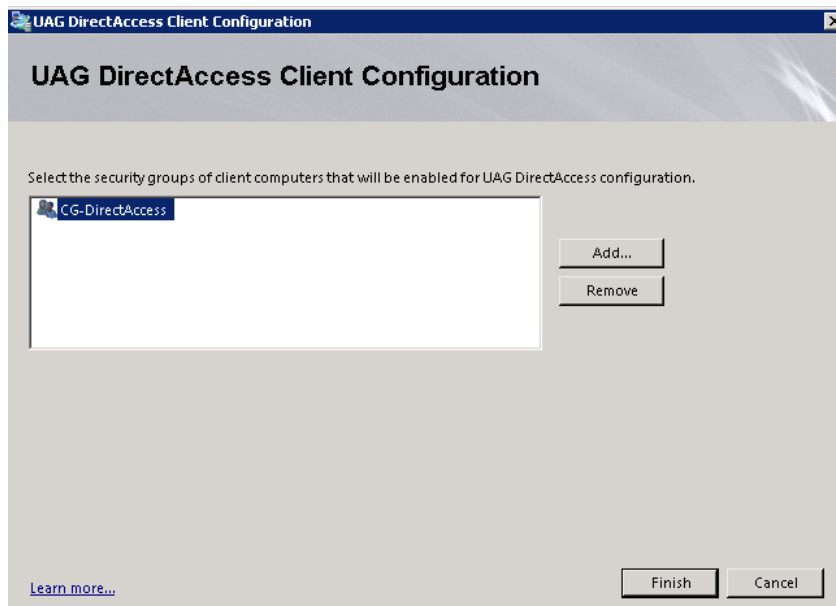
Konfiguration sichern und aktivieren



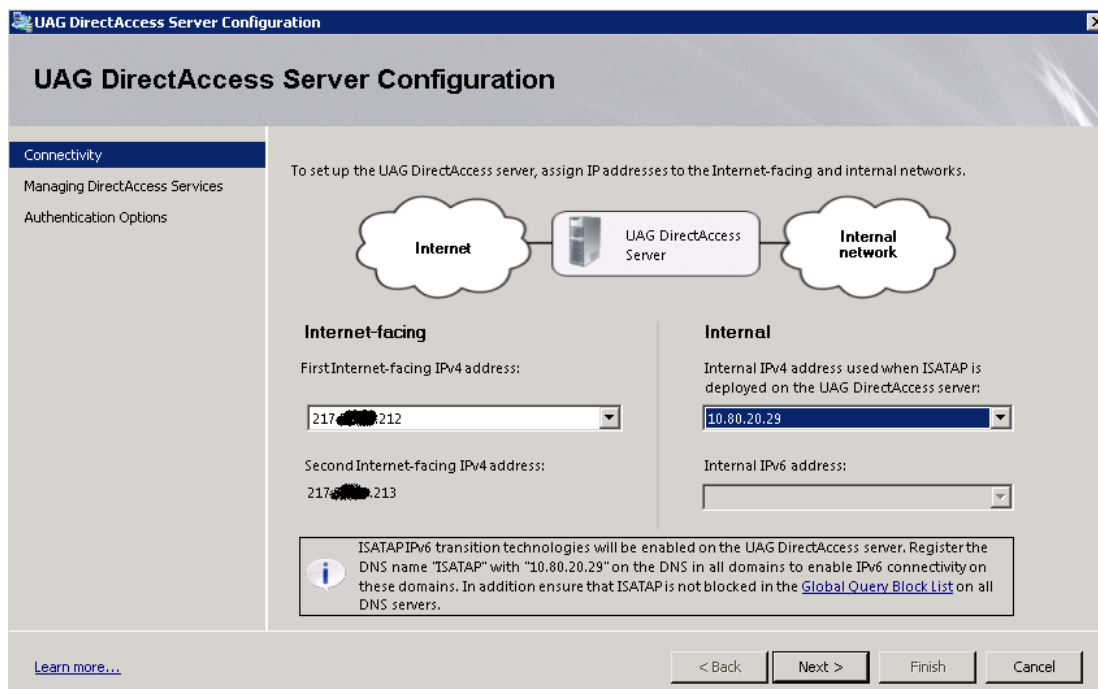
DirectAccess Einrichtung



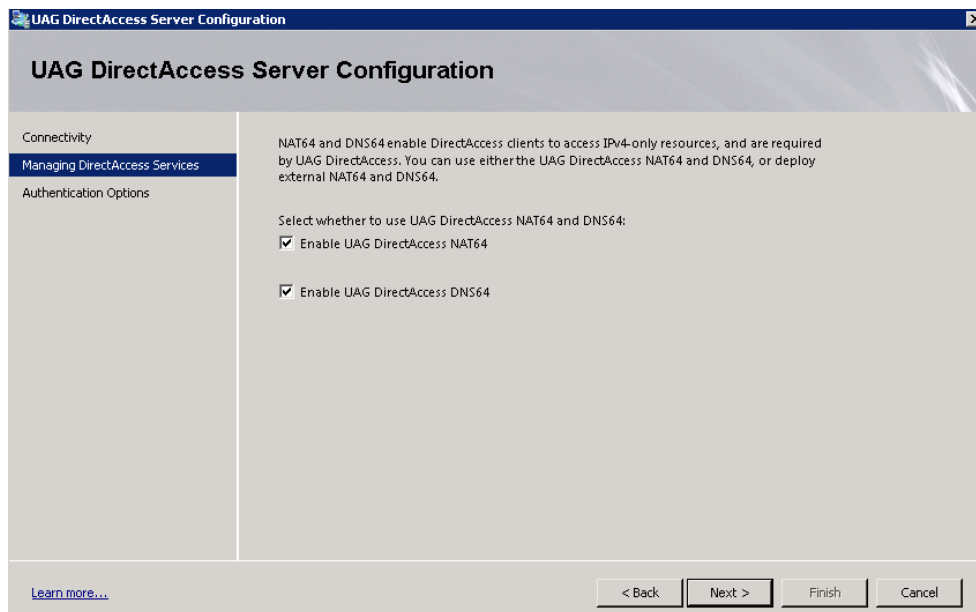
Angabe der globalen Gruppe, welche alle zukünftigen Direct Access Clients enthält. Diese Gruppe wird vom UAG DA Assistenten verwendet, um über die Sicherheitsfilterung eine erstellte Gruppenrichtlinie anzuwenden, welche für die DA-Einstellungen verwendet wird.



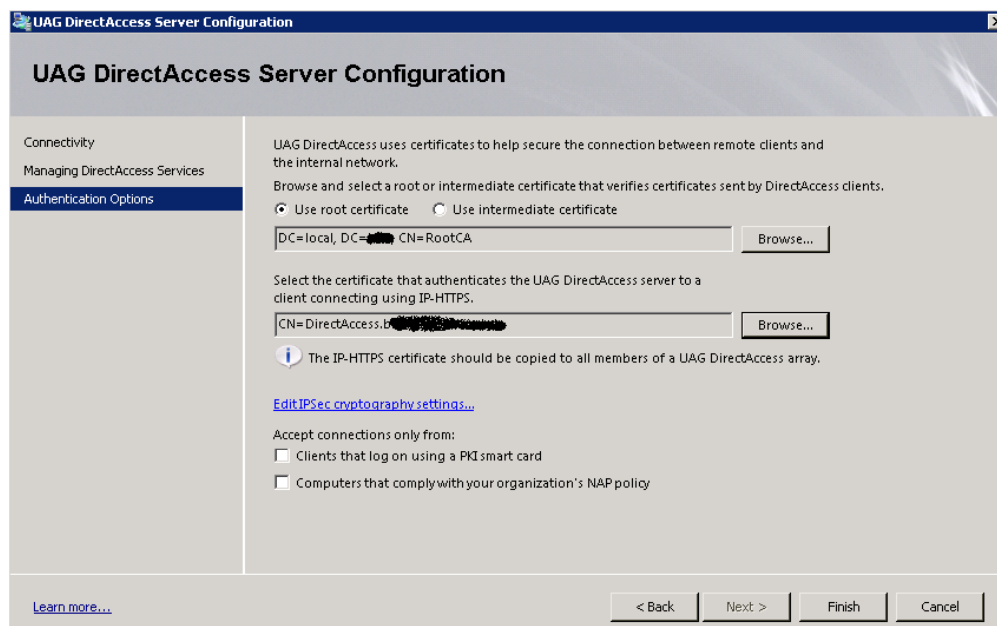
Angabe der ersten IP-Adresse, welche am externen Interface von Forefront UAG gebunden ist, auf der auch das IP-HTTPS Zertifikat gebunden ist und der Publis Hostname verweist.



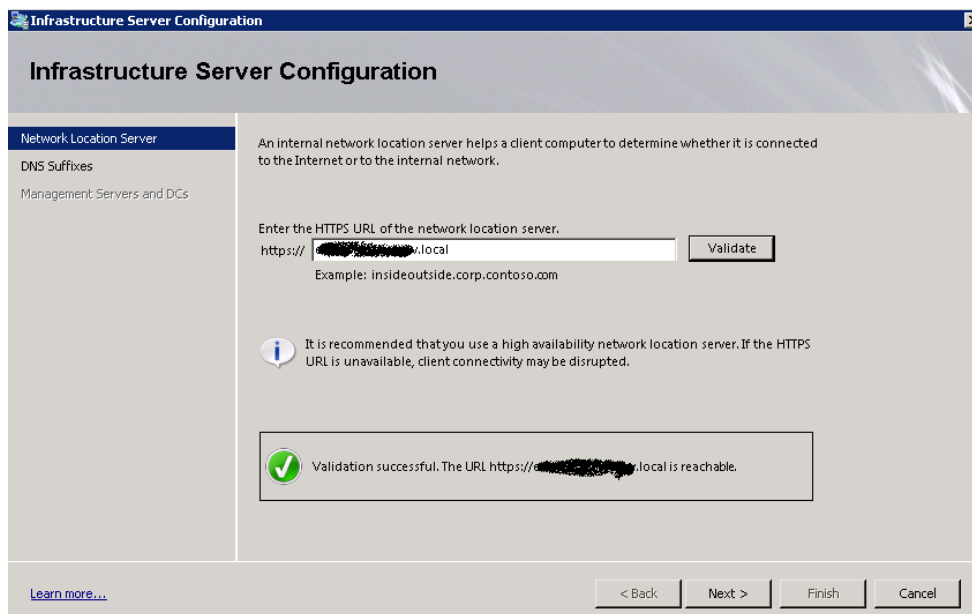
Forefront UAG fungiert als NAT64 und DNS64 Gateway / Router.



Auswahl der Root CA, welche alle Zertifikat fuer den NLS, UAG und DA Client ausgestellt hat, sowie des IP-HTTPS Zertifikats, falls der DA Client nicht per 6to4 oder Teredo connecten kann.



Angabe der URL des NLS Server



The screenshot shows the 'Infrastructure Server Configuration' window, specifically the 'Network Location Server' step. The left sidebar has 'Network Location Server' selected, with 'DNS Suffixes' and 'Management Servers and DCs' below it. The main area contains instructions: 'An internal network location server helps a client computer to determine whether it is connected to the Internet or to the internal network.' Below this is a text box for the 'HTTPS URL of the network location server' with the value 'https://[redacted].local' and a 'Validate' button. An example 'insideoutside.corp.contoso.com' is provided. A green checkmark icon indicates 'Validation successful. The URL https://[redacted].local is reachable.' At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel', along with a 'Learn more...' link.

Infrastructure Server Configuration

Network Location Server

An internal network location server helps a client computer to determine whether it is connected to the Internet or to the internal network.

Enter the HTTPS URL of the network location server.

https://[redacted].local

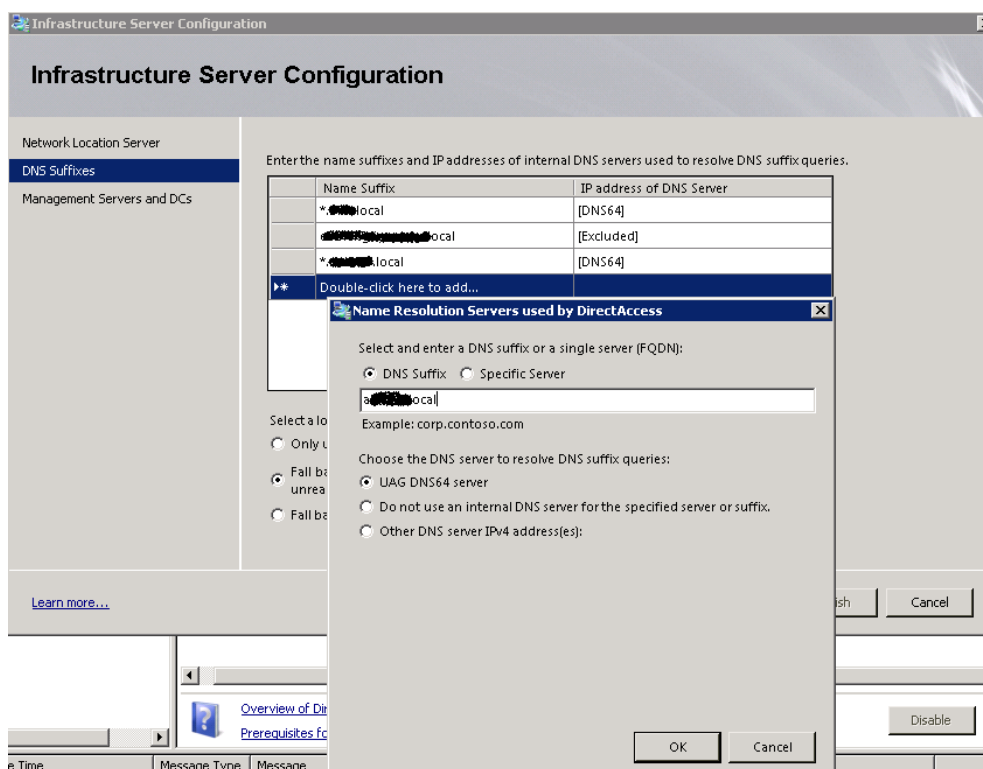
Example: insideoutside.corp.contoso.com

It is recommended that you use a high availability network location server. If the HTTPS URL is unavailable, client connectivity may be disrupted.

Validation successful. The URL https://[redacted].local is reachable.

[Learn more...](#)

Angabe der DNS Suffixe, welche vom DNS64 durch UAG dem DA Client zur Verfügung gestellt werden. Die DNS Suffixe werden in die NRPT eingetragen, so dass der DA Client weiss, fuer welche DNS Domänen er welche DNS Server verwenden soll.



The screenshot shows the 'Infrastructure Server Configuration' window, specifically the 'DNS Suffixes' step. The left sidebar has 'DNS Suffixes' selected. The main area contains instructions: 'Enter the name suffixes and IP addresses of internal DNS servers used to resolve DNS suffix queries.' Below this is a table with columns 'Name Suffix' and 'IP address of DNS Server'. The table contains three rows: '*[redacted].local' with '[DNS64]', '[redacted].local' with '[Excluded]', and '*[redacted].local' with '[DNS64]'. A 'Double-click here to add...' link is at the bottom of the table. A dialog box titled 'Name Resolution Servers used by DirectAccess' is open over the table. The dialog has two sections. The first section, 'Select and enter a DNS suffix or a single server (FQDN):', has radio buttons for 'DNS Suffix' (selected) and 'Specific Server', with a text box containing '[redacted].local' and an example 'corp.contoso.com'. The second section, 'Choose the DNS server to resolve DNS suffix queries:', has radio buttons for 'UAG DNS64 server' (selected), 'Do not use an internal DNS server for the specified server or suffix.', and 'Other DNS server IPv4 address(es):'. At the bottom of the dialog are 'OK' and 'Cancel' buttons. The background window shows the 'Finish' and 'Cancel' buttons at the bottom right.

Infrastructure Server Configuration

DNS Suffixes

Enter the name suffixes and IP addresses of internal DNS servers used to resolve DNS suffix queries.

Name Suffix	IP address of DNS Server
*[redacted].local	[DNS64]
[redacted].local	[Excluded]
*[redacted].local	[DNS64]
Double-click here to add...	

Select a local DNS server to resolve DNS suffix queries:

☐ Only use the local DNS server to resolve DNS suffix queries.

☒ Fall back to the local DNS server if the remote DNS server is unavailable.

☐ Fall back to the local DNS server if the remote DNS server is unavailable and the local DNS server is also unavailable.

Name Resolution Servers used by DirectAccess

Select and enter a DNS suffix or a single server (FQDN):

☒ DNS Suffix ☐ Specific Server

[redacted].local

Example: corp.contoso.com

Choose the DNS server to resolve DNS suffix queries:

☒ UAG DNS64 server

☐ Do not use an internal DNS server for the specified server or suffix.

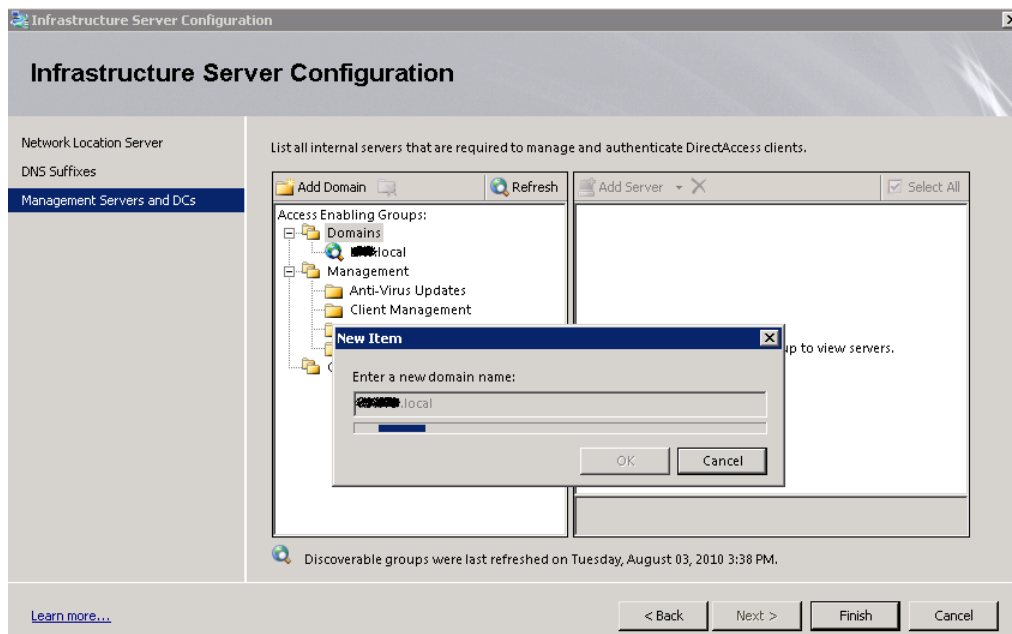
☐ Other DNS server IPv4 address(es):

OK Cancel

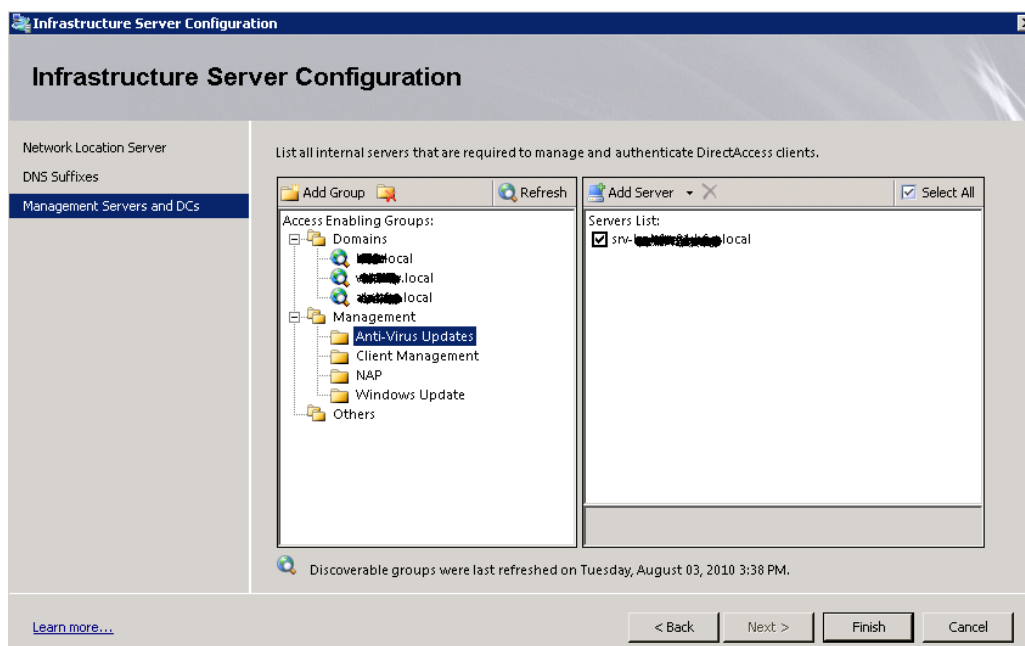
Finish Cancel

Disable

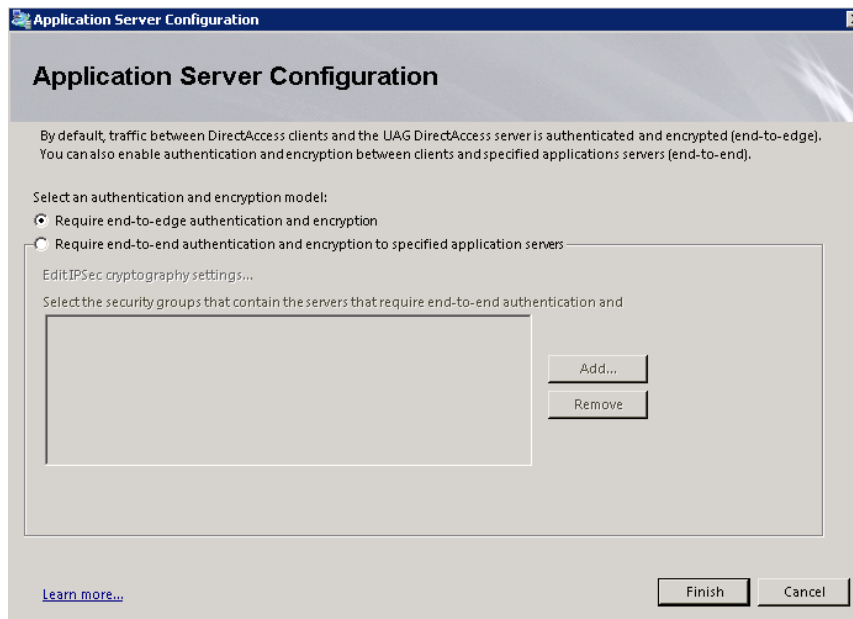
Angabe der Infrastruktur Server, welche ueber den ersten IPSEC Tunnel mit dem DA-Client kommunizieren koennen. Hierbei handelt es sich um Domaenencontroller, Virenschanner, Softwareverteilungsserver usw.



Beispiel:

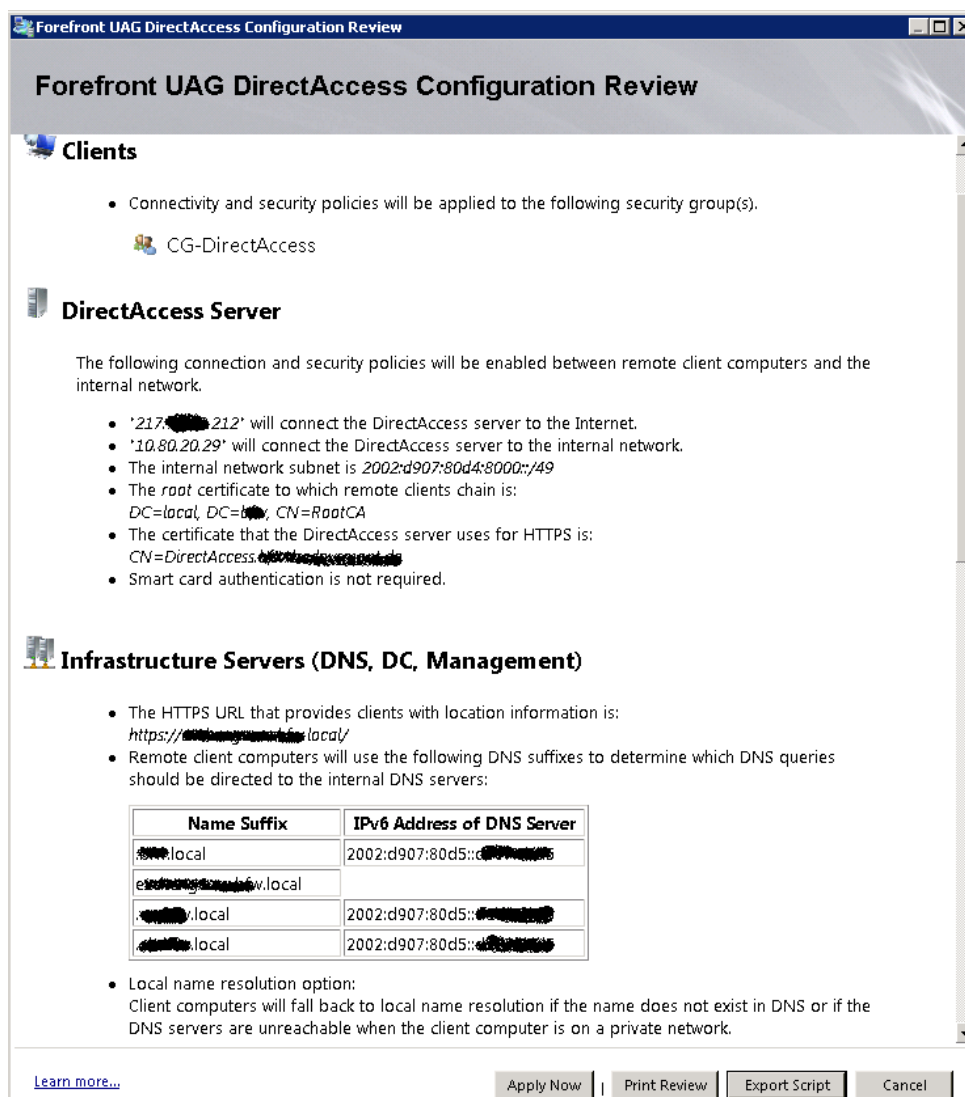


Der Zugriff auf einzelne Server im LAN kann zusaetzlich noch verschluesselt und authentifiziert werden, wenn das gewuenscht ist. Wird keine Aenderung vorgenommen, werden die Verbindungen zwischen DirectAccess Client und Forefront UAG Server authentifiziert und verschluesselt (kerberos, Computer Zertifikate, NTLMv2, AES192, DH Gruppe 2 usw.).



Konfig sichern und aktivieren

Group Policy erstellen lassen



Fuer die angegebenen Server werden auf den internen DNS Servern Ipv6 Adressen erstellt.

Forefront UAG DirectAccess Configuration Review

DNS servers are unreachable when the client computer is on a private network.

- Management servers on the following subnet(s) will be able to connect to remote client computers:

Server	IP Address/Prefix
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1402 2002:d907:80d4:8000:0:5efe:10.80.20.2
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1403 2002:d907:80d4:8000:0:5efe:10.80.20.3
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1502 2002:d907:80d4:8000:0:5efe:10.80.21.2
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1503 2002:d907:80d4:8000:0:5efe:10.80.21.3
XXXX .local	
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1002 2002:d907:80d4:8000:0:5efe:10.80.16.2
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1003 2002:d907:80d4:8000:0:5efe:10.80.16.3
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1202 2002:d907:80d4:8000:0:5efe:10.80.18.2
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1203 2002:d907:80d4:8000:0:5efe:10.80.18.3
XXXX .local	
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:2 2002:d907:80d4:8000:0:5efe:10.80.0.2
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:3 2002:d907:80d4:8000:0:5efe:10.80.0.3
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:802 2002:d907:80d4:8000:0:5efe:10.80.8.2
SRV- XXXX - XXXX .local	2002:d907:80d4:8001::a50:803 2002:d907:80d4:8000:0:5efe:10.80.8.3
Anti-Virus Updates	
srv- XXXX - XXXX .local	2002:d907:80d4:8001::a50:1406 2002:d907:80d4:8000:0:5efe:10.80.20.6
Windows Update	

[Learn more...](#) | | | |

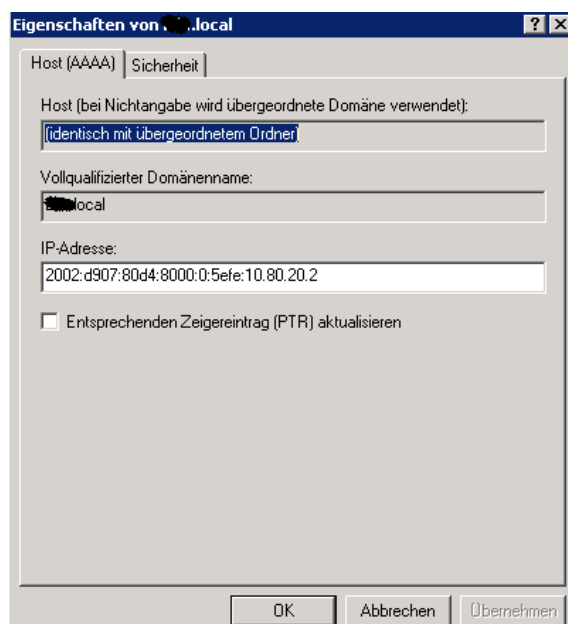
WICHTIG: Ipv6 muss in den NIC Eigenschaften der Domaenencontroller aktiviert sein. Es reicht, das Kontrollkaestchen fuer Ipv6 wieder zu aktivieren, ein Reboot ist nicht erforderlich.

Angelegte DNS Eintraege in den DNS Zonen

(identisch mit übergeordnete...	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1402
(identisch mit übergeordnete...	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1403
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1405
srv-l	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1407
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1409
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:140a
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:140f
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1410
srv-l	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1414
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1415
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1417
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:141d
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:141e
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:141f

(identisch mit übergeordnete...	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1002
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1006
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:100b
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1013
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1015
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:101c
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:101d
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:101f
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1022
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1023
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1024
SRV-	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1026
MBS	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:102b
NBK	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1046
WKS	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:1047
WKS	IPv6 Host (AAAA)	2002:d907:80d4:8000:0000:5efe:0a50:14ad

Ipv6 Adresse eines DNS Server (DC). Man beachte die Kombi Ipv4 und Ipv6 Adresse



Ggfs. Ipv6 Einstellungen auf den DNS Servern aktualisieren (nach DA Aktivierung)

sc control iphlpsvc paramchange

Erstellte GPO und Erlaeuterung

Gruppenrichtlinie UAG DirectAccess – DA Server

GPO-Status Benutzereinstellungen deaktiviert

Richtlinie	Einstellung
Richtlinienversion	2.10
Statusbehaftetes FTP deaktivieren	Nicht konfiguriert
Statusbehaftetes PPTP deaktivieren	Nicht konfiguriert
IPsec-Ausnahme	ICMP
IPsec über NAT	Nicht konfiguriert
Verschlüsselung des vorinstallierten Schlüssels	Nicht konfiguriert
SA-Leerlaufzeit	Nicht konfiguriert
Sichere Zertifikatsperrlistenprüfung	Fehler bei Sperren des Zertifikats.
Private Profileinstellungen	hide

Richtlinie	Einstellung
Firewallstatus	Ein
Eingehende Verbindungen	Nicht konfiguriert
Ausgehende Verbindungen	Nicht konfiguriert
Lokale Firewallregeln anwenden	Nicht konfiguriert
Lokale Verbindungssicherheitsregeln anwenden	Nicht konfiguriert
Benachrichtigungen anzeigen	Nicht konfiguriert
Unicast-Antworten zulassen	Nicht konfiguriert
Verworfen Pakete protokollieren	Nicht konfiguriert
Erfolgreiche Verbindungen protokollieren	Nicht konfiguriert
Protokolldateipfad	Nicht konfiguriert
Maximale Größe der Protokolldatei (KB)	Nicht konfiguriert
Öffentliche Profileinstellungen	hide

Richtlinie	Einstellung
Firewallstatus	Ein
Eingehende Verbindungen	Nicht konfiguriert
Ausgehende Verbindungen	Nicht konfiguriert
Lokale Firewallregeln anwenden	Nicht konfiguriert
Lokale Verbindungssicherheitsregeln anwenden	Nicht konfiguriert
Benachrichtigungen anzeigen	Nicht konfiguriert
Unicast-Antworten zulassen	Nicht konfiguriert
Verworfen Pakete protokollieren	Nicht konfiguriert
Erfolgreiche Verbindungen protokollieren	Nicht konfiguriert
Protokolldateipfad	Nicht konfiguriert
Maximale Größe der Protokolldatei (KB)	Nicht konfiguriert
Verbindungssicherheitseinstellungen	hide
Regeln	hide

Name	
UAG DirectAccess Gateway - Clients Access Enabling Tunnel - All	Policies to enable access granting resources(DC, DNS, NAP, etc.) over IPsec. Generated on Tuesday, 03 August 2010 14:15 UTC.
Aktiviert	Wahr
Authentifizierungsmodus	Eingehend und ausgehend erforderlich 2002:d907:80d4:8001::a50:1402, 2002:d907:80d4:8000:0:5efe:10.80.20.2, 2002:d907:80d4:8001::a50:1403, 2002:d907:80d4:8000:0:5efe:10.80.20.3, 2002:d907:80d4:8001::a50:1502, 2002:d907:80d4:8000:0:5efe:10.80.21.2, 2002:d907:80d4:8001::a50:1503, 2002:d907:80d4:8000:0:5efe:10.80.21.3, 2002:d907:80d4:8001::a50:1002, 2002:d907:80d4:8000:0:5efe:10.80.16.2, 2002:d907:80d4:8001::a50:1003, 2002:d907:80d4:8000:0:5efe:10.80.16.3, 2002:d907:80d4:8001::a50:1202, 2002:d907:80d4:8000:0:5efe:10.80.18.2, 2002:d907:80d4:8001::a50:1203, 2002:d907:80d4:8000:0:5efe:10.80.18.3, 2002:d907:80d4:8001::a50:2, 2002:d907:80d4:8000:0:5efe:10.80.0.2, 2002:d907:80d4:8001::a50:3, 2002:d907:80d4:8000:0:5efe:10.80.0.3, 2002:d907:80d4:8001::a50:802, 2002:d907:80d4:8000:0:5efe:10.80.8.2, 2002:d907:80d4:8001::a50:803, 2002:d907:80d4:8000:0:5efe:10.80.8.3, 2002:d907:80d4:8001::a50:1406, 2002:d907:80d4:8000:0:5efe:10.80.20.6, 2002:d907:80d4:8001::a50:1402, 2002:d907:80d4:8000:0:5efe:10.80.20.2, 2002:d907:80d5::d907:80d5
Endpunkt 1	
Endpunkt 2	Beliebig
Endpunkt 1 (Port)	Beliebig
Endpunkt 2 (Port)	Beliebig
Erste Authentifizierung	{C3D8F907-29F8-4356-A64C-570950685CC5}
Zweite Authentifizierung	{DD5FBEF2-4438-4CEC-81C4-169B50E66418}
Datenschutz	{7487C8D9-E9E5-4C1D-9012-3166FFEDCB49}
Protokoll	Beliebig
Profil	Privat, Öffentlich
Tunnelendpunkt 1	Beliebig
Tunnelendpunkt 2	Beliebig
Netzwerkschnittstellentyp	Beliebig

Aktiviert	Wahr
Authentifizierungsmodus	Eingehend und ausgehend erforderlich
Endpunkt 1	2002:d907:80d4:8000::/49
Endpunkt 2	Beliebig
Endpunkt 1 (Port)	Beliebig
Endpunkt 2 (Port)	Beliebig
Erste Authentifizierung	{EA98A748-D882-491C-958D-9ACE7395FEB0}
Zweite Authentifizierung	{5A830407-7E7E-4943-9F81-90BB65F71061}
Datenschutz	{F98D74C6-8DD6-410B-A372-E66CDA8DDD61}
Protokoll	Beliebig
Profil	Privat, Öffentlich
Tunnelendpunkt 1	Beliebig
Tunnelendpunkt 2	Beliebig
Netzwerkschnittstellentyp	Beliebig
Erste Authentifizierung	

Name	Beschreibung
UAG DirectAccess Gateway - Clients Access Enabling Tunnel - All - Phase 1	
Auth Set {C3D8F907-29F8-4356-A64C-570950685CC5}	
Version	2.10
Authentifizierung	Computerzertifikat
Zertifizierungsstelle	DC=local, DC=xxx, CN=RootCA
Zertifizierungsstellenzuordnung	Falsch
Ausgeschlossene Zertifizierungsstelle	Falsch
Integritätszertifikat	Falsch

Name	Beschreibung
UAG DirectAccess Gateway - Clients Corp Tunnel - Phase 1 Auth Set	
{EA98A748-D882-491C-958D-9ACE7395FEB0}	
Version	2.10
Authentifizierung	Computerzertifikat
Zertifizierungsstelle	DC=local, DC=xxx, CN=RootCA
Zertifizierungsstellenzuordnung	Falsch
Ausgeschlossene Zertifizierungsstelle	Falsch
Integritätszertifikat	Falsch
Zweite Authentifizierung	

Name	Beschreibung
UAG DirectAccess Gateway - Clients Corp Tunnel - Phase 2 Auth Set {5A830407-7E7E-4943-9F81-90BB65F71061}	
Version	2.10
Authentifizierung	Benutzer (Kerberos)

Name	Beschreibung
UAG DirectAccess Gateway - Clients Access Enabling Tunnel - All - Phase 2 Auth Set {DD5FBEF2-4438-4CEC-81C4-169B50E66418}	
Version	2.10
Authentifizierung	Benutzer-NTLM
Schlüsselaustausch (Hauptmodus)	

Name	Beschreibung
Standardsatz	
Version	2.10
Schlüsselgültigkeitsdauer (in Minuten)	60
Schlüsselgültigkeitsdauer in Sitzungen	0
Version überspringen	2.0
Schlüsselaustausch	Diffie-Hellman-Gruppe 2
Verschlüsselung	AES-128
Integrität	MD5
Version überspringen	0.0
Schlüsselaustausch	Diffie-Hellman-Gruppe 2
Verschlüsselung	AES-128
Integrität	SHA-1
Version überspringen	0.0
Schlüsselaustausch	Diffie-Hellman-Gruppe 2
Verschlüsselung	3DES
Integrität	SHA-1
Datenschutz (Schnellmodus)	

Name	Beschreibung
UAG DirectAccess Gateway - Clients Access Enabling Tunnel - All - Phase 2 Crypto Set {7487C8D9-E9E5-4C1D-9012-3166FFEDCB49}	
Version	2.10
Perfect Forward Secrecy	Deaktiviert
Version überspringen	0.0
Protokoll	ESP
Verschlüsselung	AES-192
ESP-Integrität	SHA-1
Schlüsselgültigkeitsdauer (in Minuten)	60
Schlüsselgültigkeitsdauer (in Kilobyte)	100000

Name	Beschreibung
UAG DirectAccess Gateway - Clients Corp Tunnel - Phase 2 Crypto Set {F98D74C6-8DD6-410B-A372-E66CDA8DDD61}	
Version	2.10
Perfect Forward Secrecy	Deaktiviert
Version überspringen	0.0
Protokoll	ESP
Verschlüsselung	AES-192
ESP-Integrität	SHA-1
Schlüsselgültigkeitsdauer (in Minuten)	60
Schlüsselgültigkeitsdauer (in Kilobyte)	100000
Benutzerkonfiguration (Deaktiviert) hide	
Keine Einstellungen definiert	

Gruppenrichtlinie UAG DirectAccess - Client

NLS

JAG DirectAccess: Client{3491980e-ef3c-4ed3-b176-a4420a810f12}

Bereich | Details | Einstellungen | Delegation |

Die Liste sollte durch Kommas getrennt sein und keine zusätzlichen Leerzeichen aufweisen.
Beispiel:
fe80::/9,fe81::/9

Richtlinie	Einstellung	Kommentar
Testhostadresse für Firmen-DNS	Aktiviert	
Testadresse für Firmen-DNS:	::1	
Geben Sie die erwartete DNS-Adresse für den zu testenden Firmenhostnamen an. Beispiel: 2001:4898:28:3:38a1:c31:7b3d:bf0		

Richtlinie	Einstellung	Kommentar
Testhostname für Firmen-DNS	Aktiviert	
Testhostname des Firmen-DNS:	UAGDirectAccess-corpConnectivityHost.192.168.1.100.local	
Geben Sie einen aufzulösenden Firmenhostnamen zum Testen der Unternehmenskonnektivität an. Beispiel: ncsi.corp.microsoft.com		

Richtlinie	Einstellung	Kommentar
URL zur Bestimmung des Domänenorts	Aktiviert	
URL zur Bestimmung des Firmendomänenorts:	https://192.168.1.100.local/	
Geben Sie die HTTPS-URL der Firmenwebsite an, um den Domänenort inner- oder außerhalb zu ermitteln. Beispiel: https://nid.corp.microsoft.com/		

Netzwerk/TCP/IP-Einstellungen/IPv6-Übergangstechnologien [show](#)

Zusätzl. Reg.-einst. [show](#)

NRPT fuer den DA Client

Group Policy Management Editor

File Action View Help

UAG DirectAccess: Client{34...}

Computer Configuration

Policies

Software Settings

Windows Settings

Name Resolution Policy Table (NRPT)

Scripts (Star...)

Security Settings

Policy-based Administrative Templates

Preferences

User Configuration

Policies

Preferences

The Name Resolution Policy Table (NRPT) stores configuration settings for DNS security (DNSSEC) and Direct Access on DNS client computers. You can use this page to create or edit rules, which are used to make policies that can be applied to an Active Directory organizational unit (OU).

[Learn more about DNSSEC on the Web](#)

Description

Name Resolution Policy is the Group Policy object (GPO) that contains the policy information found in the Name Resolution Policy Table (NRPT).

Create Rules

To which part of the namespace does this rule apply?

Suffix: local

Certification authority: (Optional) DC=local, DC=local, CN=RootCA Browse...

DNSSEC DNS Settings for Direct Access

☒ Enable DNS settings for Direct Access in this rule

DNS settings for Direct Access

DNS servers (optional): 2002:d907:80d5::d907:80d5 Add... Edit... Remove

Web proxy (optional):
☐ Use this Web proxy:
☒ Use the default Web proxy

IPsec:
☐ Use IPsec in communication between the DNS client and DNS server
Encryption type: No encryption (integrity only)

Update Create Clear

Advanced Global Policy Settings

Name Resolution Policy Table

Namespace	CA	DNSSEC (V...	DNSSEC (I...	DNSSEC (I...	Direct Acce...	Direct Acce...	Direct Acce...	Direct Acce...
local	DC=lo...				2002:d907:...		No	
local	DC=lo...				2002:d907:...		No	
local	DC=lo...				2002:d907:...		No	
local	DC=lo...				2002:d907:...		No	

Delete Rule Edit Rule

Apply Cancel

Namespace

JAG DirectAccess: Client{3491980e-ef3c-4ed3-b176-a4420a810f12}

Bereich | Details | Einstellungen | Delegierung

Regeleinstellungen hide

Namespace

Richtlinie	Wert
Namespace	...local
Zertifizierungsstelle	DC=local, DC=..., CN=RootCA
Konfiguration	Direktzugriff
DNSSEC (Überprüfung)	Nicht konfiguriert
DNSSEC (IPsec)	Nicht konfiguriert
DNSSEC (IPsec-Verschlüsselung)	Nicht konfiguriert
Direktzugriff (IPsec)	Nein
Direktzugriff (IPsec-Verschlüsselung)	Keine Verschlüsselung (nur Integrität)
Direktzugriff (Proxyeinstellungen)	Keinen Webproxy verwenden
Direktzugriff (Webproxy)	Leer
Direktzugriff (DNS-Server)	2002:d907:80d5::d907:80d5
Version	1

...v.local

Richtlinie	Wert
Namespace	...local
Zertifizierungsstelle	DC=local, DC=..., CN=RootCA
Konfiguration	Direktzugriff
DNSSEC (Überprüfung)	Nicht konfiguriert
DNSSEC (IPsec)	Nicht konfiguriert
DNSSEC (IPsec-Verschlüsselung)	Nicht konfiguriert
Direktzugriff (IPsec)	Nein
Direktzugriff (IPsec-Verschlüsselung)	Keine Verschlüsselung (nur Integrität)
Direktzugriff (Proxyeinstellungen)	Keinen Webproxy verwenden
Direktzugriff (Webproxy)	Leer
Direktzugriff (DNS-Server)	Leer
Version	1

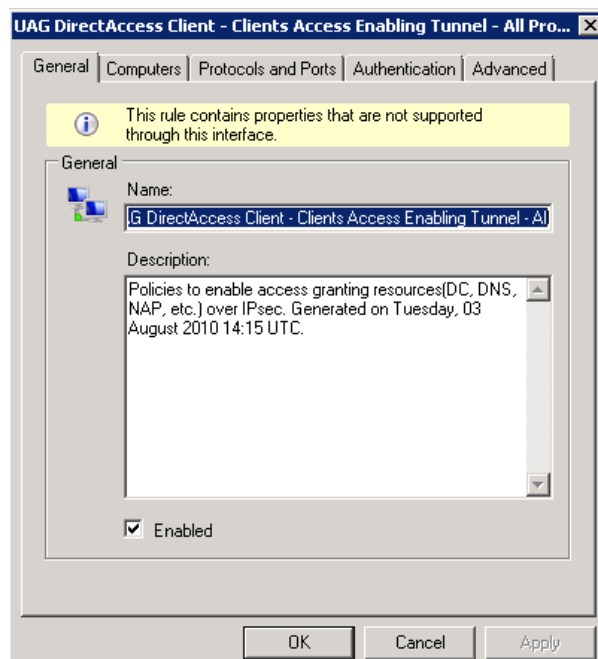
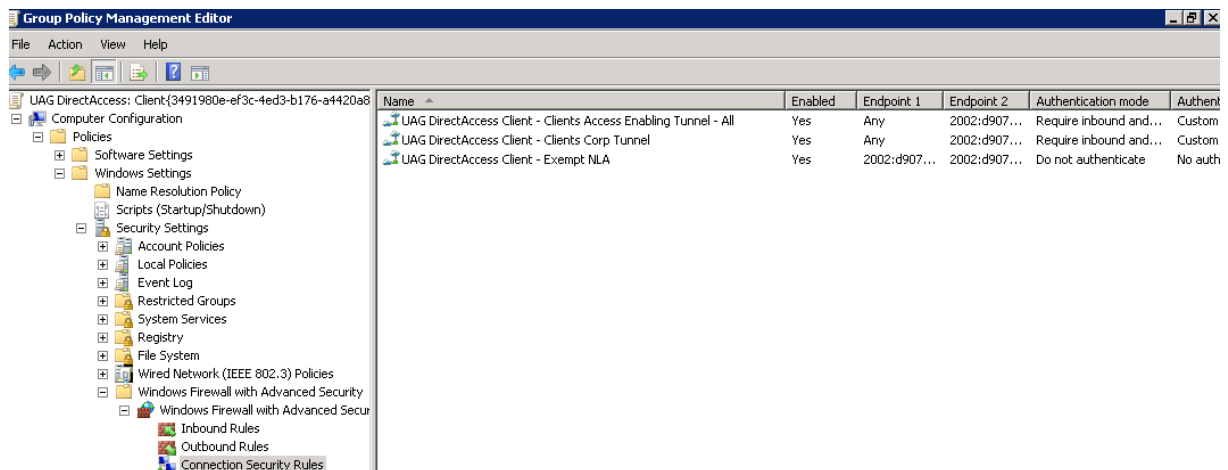
...cal

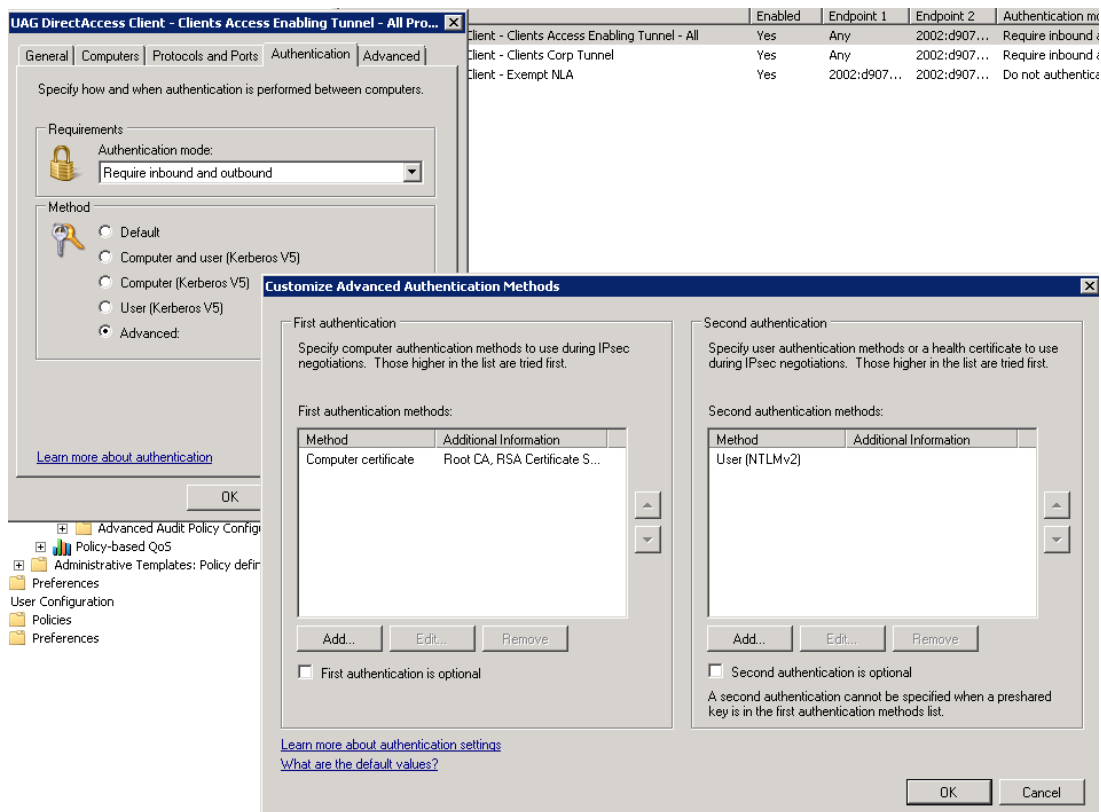
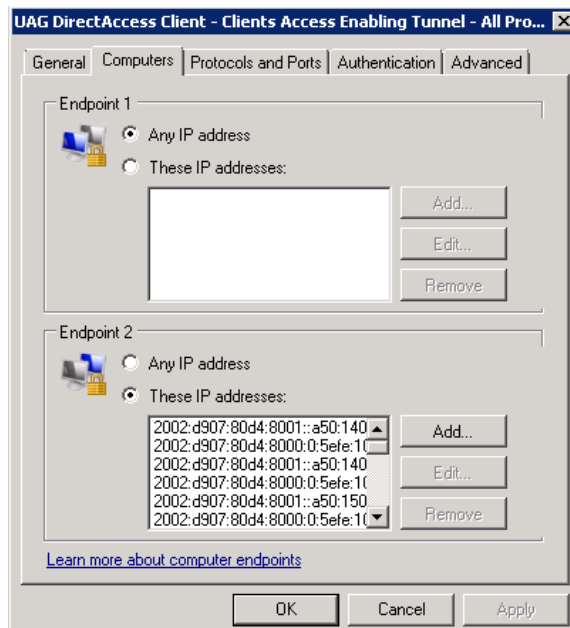
Richtlinie	Wert
Namespace	...local
Zertifizierungsstelle	DC=local, DC=..., CN=RootCA
Konfiguration	Direktzugriff
DNSSEC (Überprüfung)	Nicht konfiguriert
DNSSEC (IPsec)	Nicht konfiguriert
DNSSEC (IPsec-Verschlüsselung)	Nicht konfiguriert
Direktzugriff (IPsec)	Nein
Direktzugriff (IPsec-Verschlüsselung)	Keine Verschlüsselung (nur Integrität)
Direktzugriff (Proxyeinstellungen)	Keinen Webproxy verwenden

WICHTIG: Den TEREDO Adapter per GPO auf „Enterprise Client“ setzen, damit in einem Domain Managed Network zuerst Teredo verwendet und nicht auf IP-HTTPS geschwenkt wird:

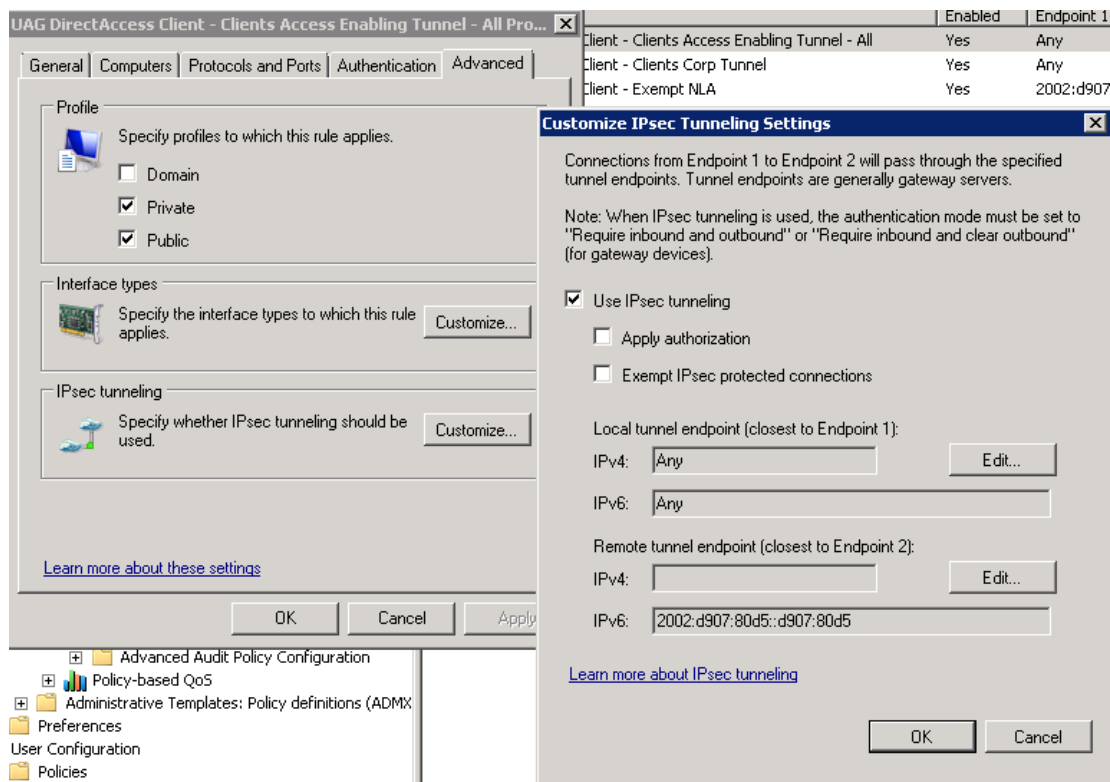
<http://blogs.technet.com/b/edgeaccessblog/archive/2010/05/21/directaccess-and-teredo-adapter-behavior.aspx>

Connection Security Rules fuer die DirectAccess Clients

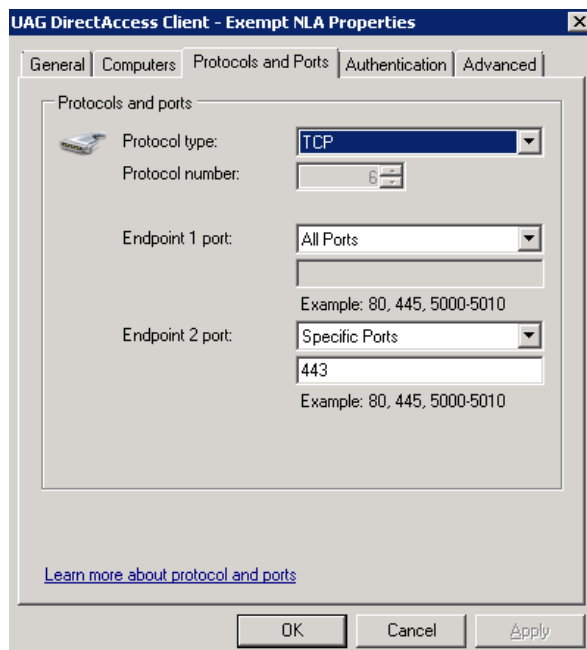




IPSEC Endpunkte



NLA Ausnahmen fuer NLS Server



Computerzertifikat fuer Windows 7 Client

Fuer die DA Clients muss ein Computerzertifikat der vertrauenswuerdigen Zertifizierungsstelle ausgestellt werden, welche auch von Forefront UAG und dem NLS verwendet wird.

CN = Interner DNS FQDN der Clients

Ueberpruefung der Ipv6 Konnektivitaet auf dem UAG Server

```
Host Name . . . . . : SRV-xxx-xxx
Primary Dns Suffix . . . . . : xxx.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : Yes
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : xxx.local
```

Ethernet adapter Local Area Connection:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : SSL Network Tunneling
Physical Address. . . . . : 00-FF-08-01-19-47
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

Ethernet adapter INTERNAL:

```

Connection-specific DNS Suffix  . : xxx.local
Description . . . . . : Broadcom BCM5708S NetXtreme II GigE (NDIS VBD
Client)
Physical Address. . . . . : 00-1A-64-32-7C-28
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::114e:2cc8:f287:ed65%11(Preferred)
IPv4 Address. . . . . : 10.80.20.29(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 234887780
DHCPv6 Client DUID. . . . . : 00-01-00-01-13-E8-71-9E-00-1A-64-32-7C-28
DNS Servers . . . . . : 10.80.20.2
                        10.80.20.3
NetBIOS over Tcpip. . . . . : Enabled

```

Ethernet adapter EXTERNAL:

```

Connection-specific DNS Suffix . : 
Description . . . . . : Broadcom BCM5708S NetXtreme II GigE (NDIS VBD
Client) #2
Physical Address. . . . . : 00-1A-64-32-7C-26
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::d5e0:d210:51c2:7422%12(Preferred)
IPv4 Address. . . . . : 217.x.xxx.212(Preferred)
Subnet Mask . . . . . : 255.255.255.240
IPv4 Address. . . . . : 217.x.xxx.213(Preferred)
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . : 217.x.xxx.217

```

DHCPv6 IAID : 301996644
DHCPv6 Client DUID. : 00-01-00-01-13-E8-71-9E-00-1A-64-32-7C-28
DNS Servers : fec0:0:0:ffff::1%1
 fec0:0:0:ffff::2%1
 fec0:0:0:ffff::3%1
NetBIOS over Tcpi. : Disabled

Tunnel adapter 6TO4 Adapter:

Connection-specific DNS Suffix . :
Description : Microsoft 6to4 Adapter
Physical Address. : 00-00-00-00-00-00-E0
DHCP Enabled. : No
Autoconfiguration Enabled . . . : Yes
IPv6 Address. : 2002:d907:80d4::d907:80d4(Preferred)
IPv6 Address. : 2002:d907:80d5::d907:80d5(Preferred)
Default Gateway : 2002:c058:6301::c058:6301
DNS Servers : fec0:0:0:ffff::1%1
 fec0:0:0:ffff::2%1
 fec0:0:0:ffff::3%1
NetBIOS over Tcpi. : Disabled

Tunnel adapter Local Area Connection* 9:

Connection-specific DNS Suffix . :
Description : Teredo Tunneling Pseudo-Interface
Physical Address. : 00-00-00-00-00-00-E0
DHCP Enabled. : No
Autoconfiguration Enabled . . . : Yes
Link-local IPv6 Address : fe80::8000:f227:26f8:7f2b%13(Preferred)
Default Gateway :
NetBIOS over Tcpi. : Disabled

Tunnel adapter isatap.xxx.local:

Connection-specific DNS Suffix . : xxx.local
Description : Microsoft ISATAP Adapter
Physical Address. : 00-00-00-00-00-00-E0
DHCP Enabled. : No
Autoconfiguration Enabled . . . : Yes
IPv6 Address. : 2002:d907:80d4:8000:0:5efe:10.80.20.29(Preferred)
Link-local IPv6 Address : fe80::5efe:10.80.20.29%16(Preferred)
Default Gateway :
DNS Servers : 10.80.20.2
 10.80.20.3
NetBIOS over Tcpi. : Disabled

Tunnel adapter isatap.{C36EA179-74B6-4982-A670-1866E35A968F}:

Connection-specific DNS Suffix . :
Description : Microsoft ISATAP Adapter #2

Physical Address. : 00-00-00-00-00-00-E0
DHCP Enabled. : No
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::200:5efe:217.7.128.212%17(Preferred)
Link-local IPv6 Address : fe80::200:5efe:217.7.128.213%17(Preferred)
Default Gateway :
DNS Servers : fec0:0:0:ffff::1%1
 fec0:0:0:ffff::2%1
 fec0:0:0:ffff::3%1
NetBIOS over Tcpip. : Disabled

Tunnel adapter IPHTTPSInterface:

Connection-specific DNS Suffix . :
Description : IPHTTPSInterface
Physical Address. : 00-00-00-00-00-00-E0
DHCP Enabled. : No
Autoconfiguration Enabled : Yes
IPv6 Address. : 2002:d907:80d4:8100:44ca:3c67:31f2:48c4(Preferred)
Link-local IPv6 Address : fe80::44ca:3c67:31f2:48c4%18(Preferred)
Default Gateway :
NetBIOS over Tcpip. : Disabled

Tunnel adapter isatap.{BCE2BA7D-B251-480A-97C6-24DECBFC7FFC}:

Media State : Media disconnected
Connection-specific DNS Suffix . :
Description : Microsoft ISATAP Adapter #3
Physical Address. : 00-00-00-00-00-00-E0
DHCP Enabled. : No
Autoconfiguration Enabled : Yes

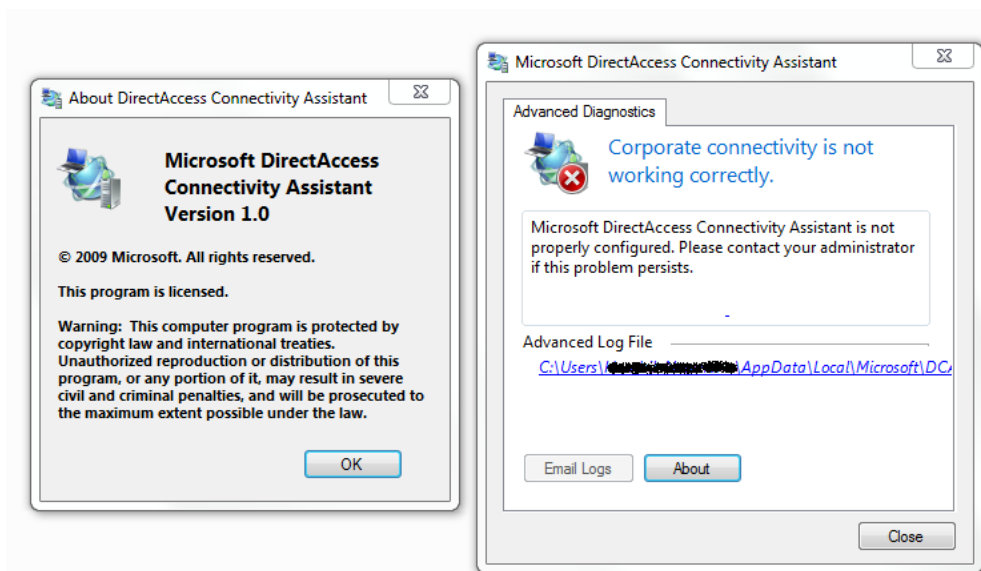
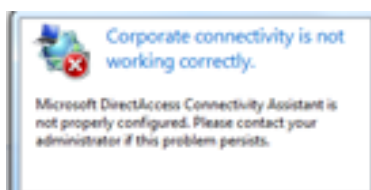
Troubleshooting

DirectAccess Troubleshooting Assistant

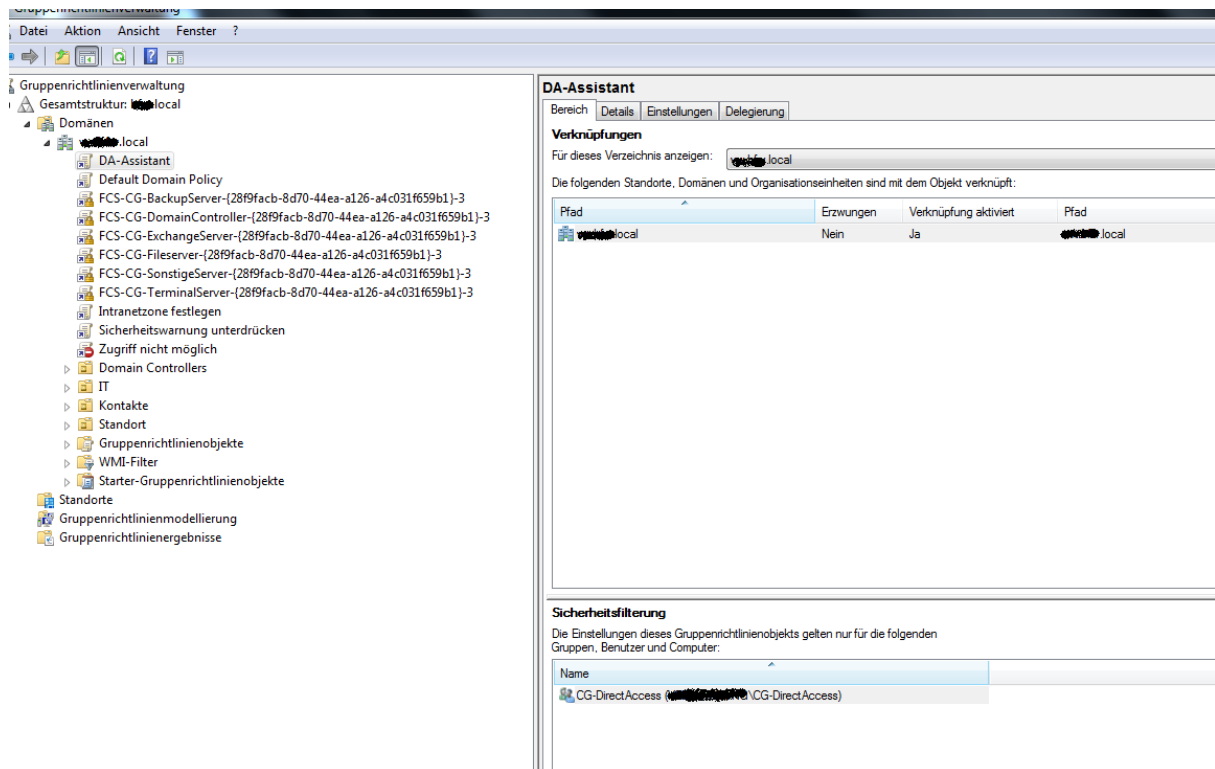
<http://www.microsoft.com/downloads/details.aspx?FamilyID=9A87EFE8-E254-4473-8A26-678ADEA6D9E9&displaylang=en>



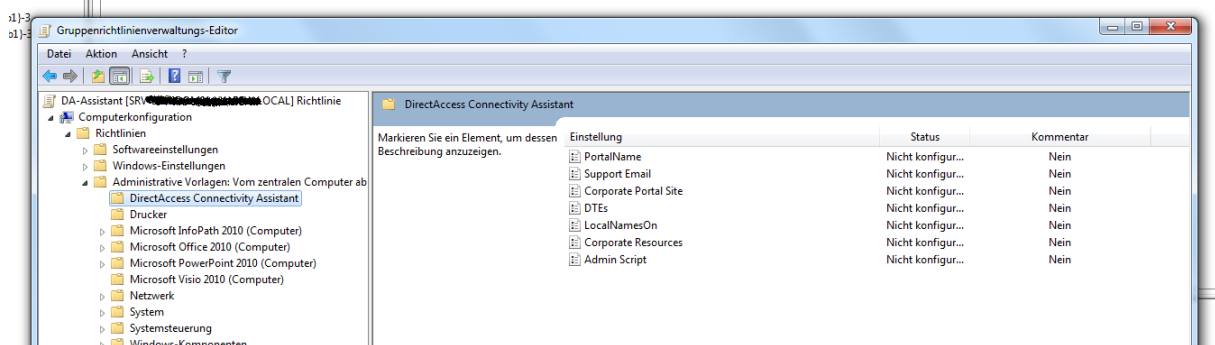
Brille aufsetzen



DA Assistant – GPO Einstellungen



Die moeglichen Einstellungen sind in dem DA Assistenten Word Dokument erlaeutert



Client Experience

Alles Gut, always on ☺

