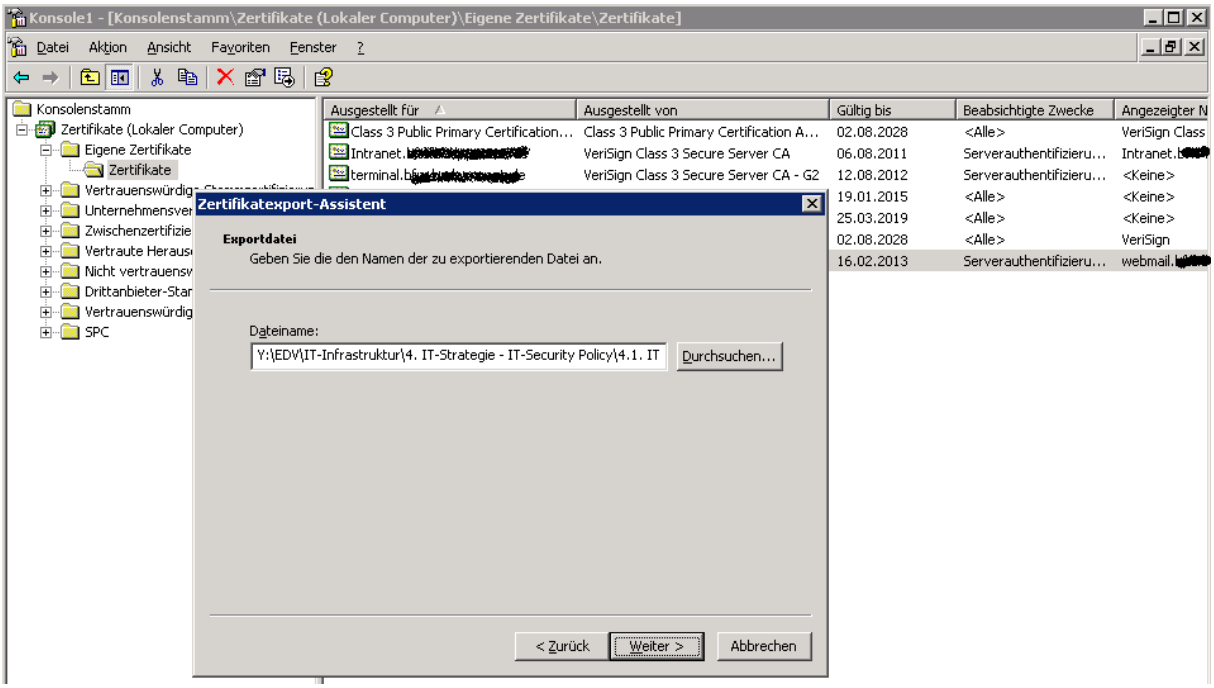
Forefront TMG EE Migration von ISA Server 2006 EE

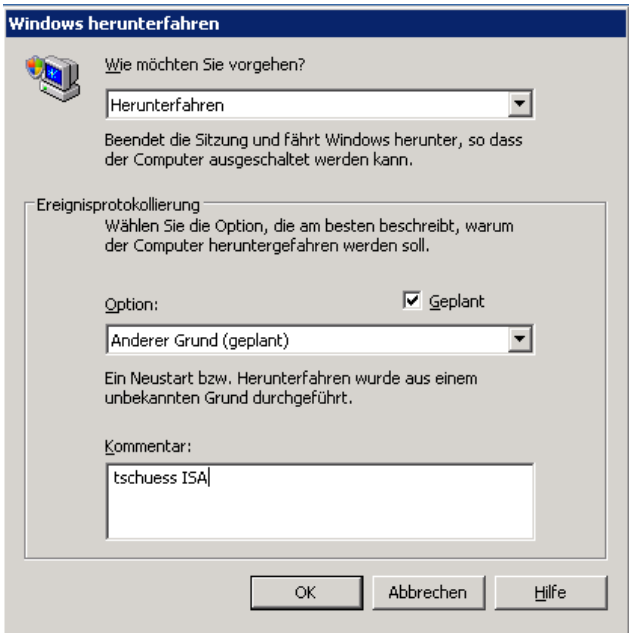
Erste Schritte

- Backup der ISA Server Konfiguration
- Ueberarbeitung und ggfs. Anpassung des Regelwerks
- Export der ISA Server Zertifikate
- Dokumentation der Netzwerkkarten und –Einstellungen
- Dokumentation erstellter Netzwerkrouten

Zertifikate exportieren

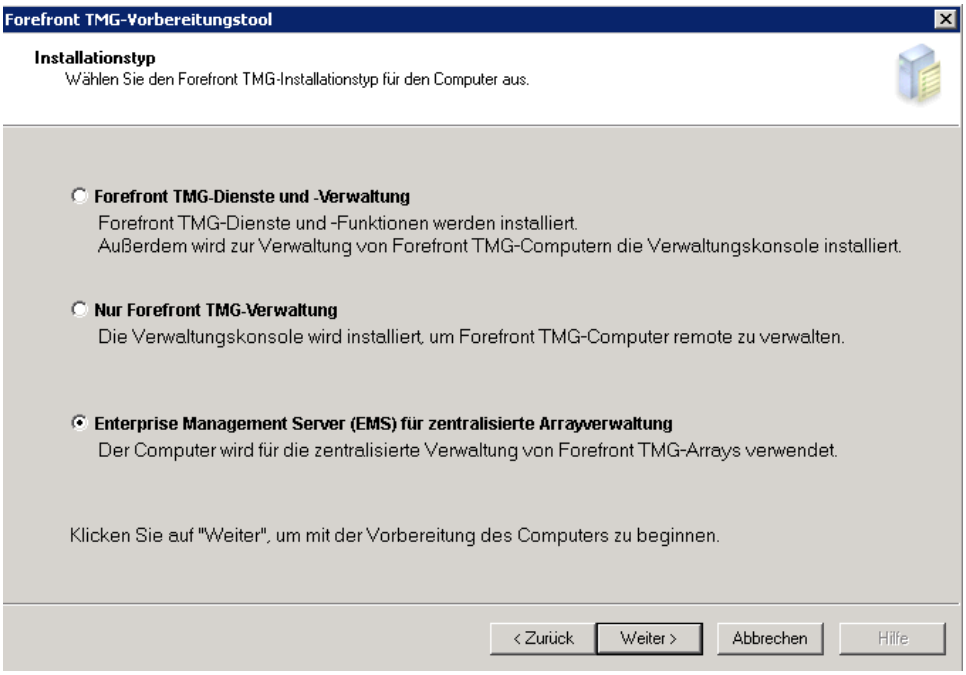


ISA Server herunterfahren

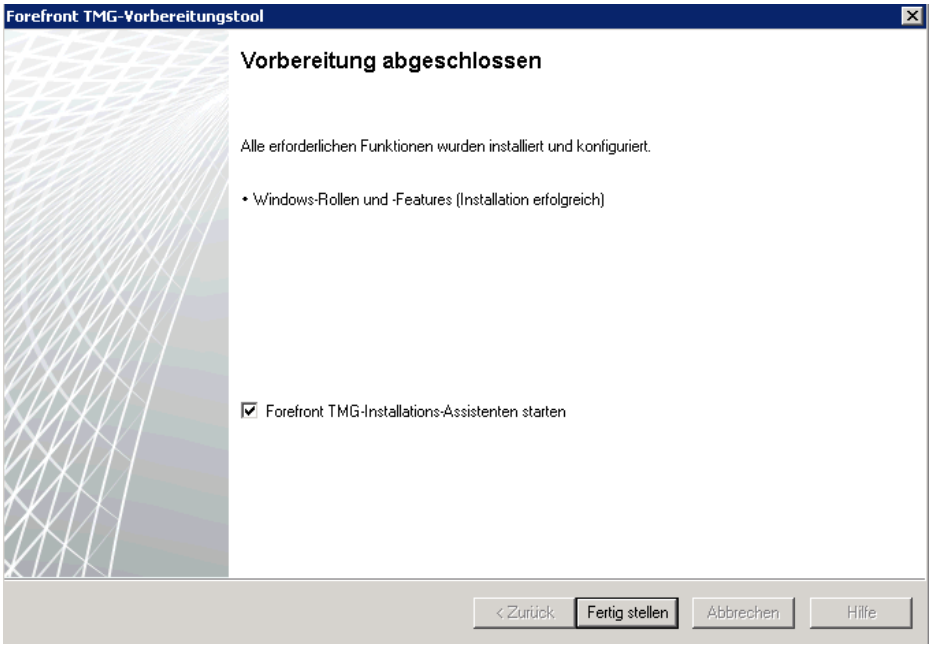


EMS Installation

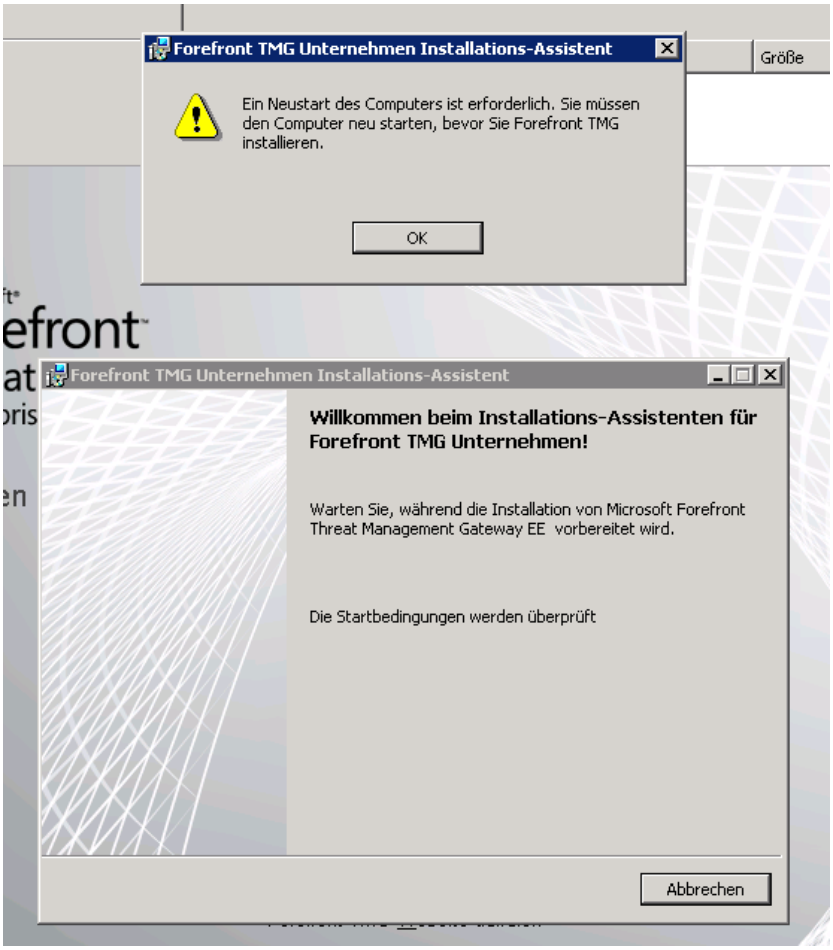
Vorbereitungstools ausfuehren



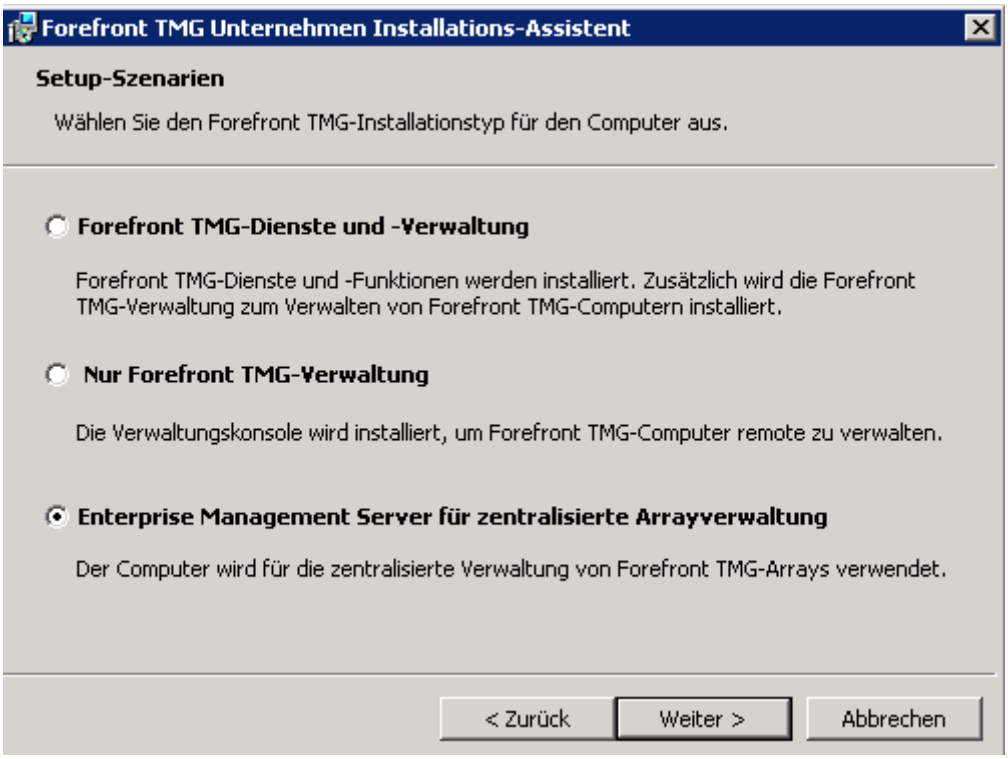
Installationsassistenten starten



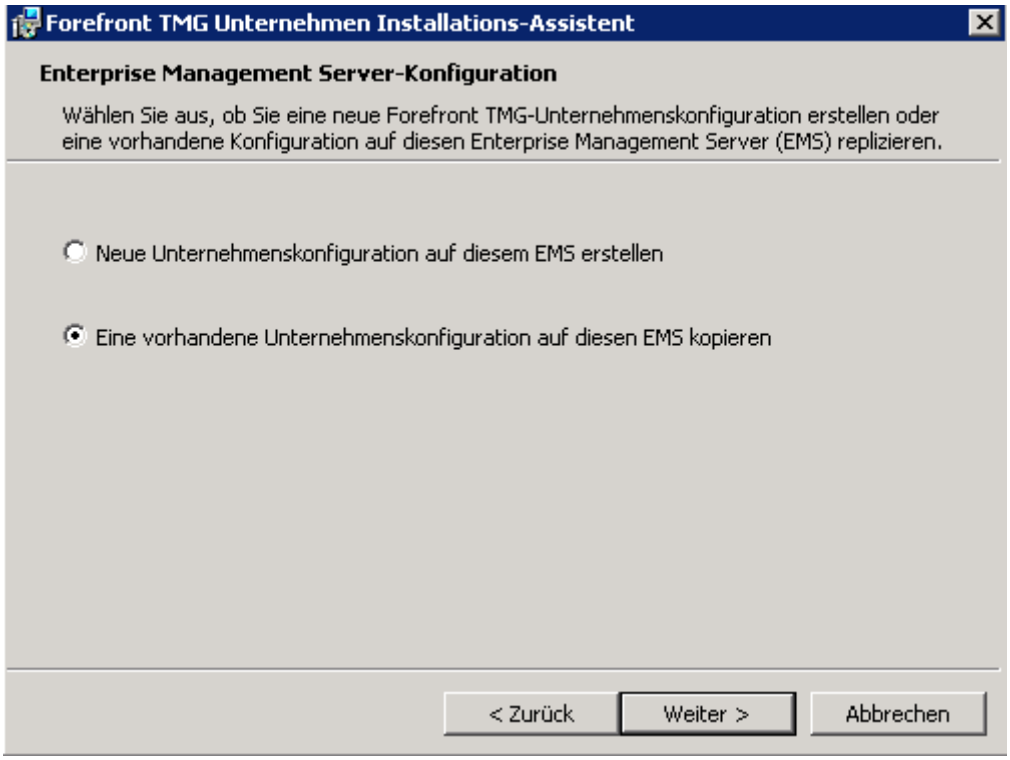
Neustart erforderlich



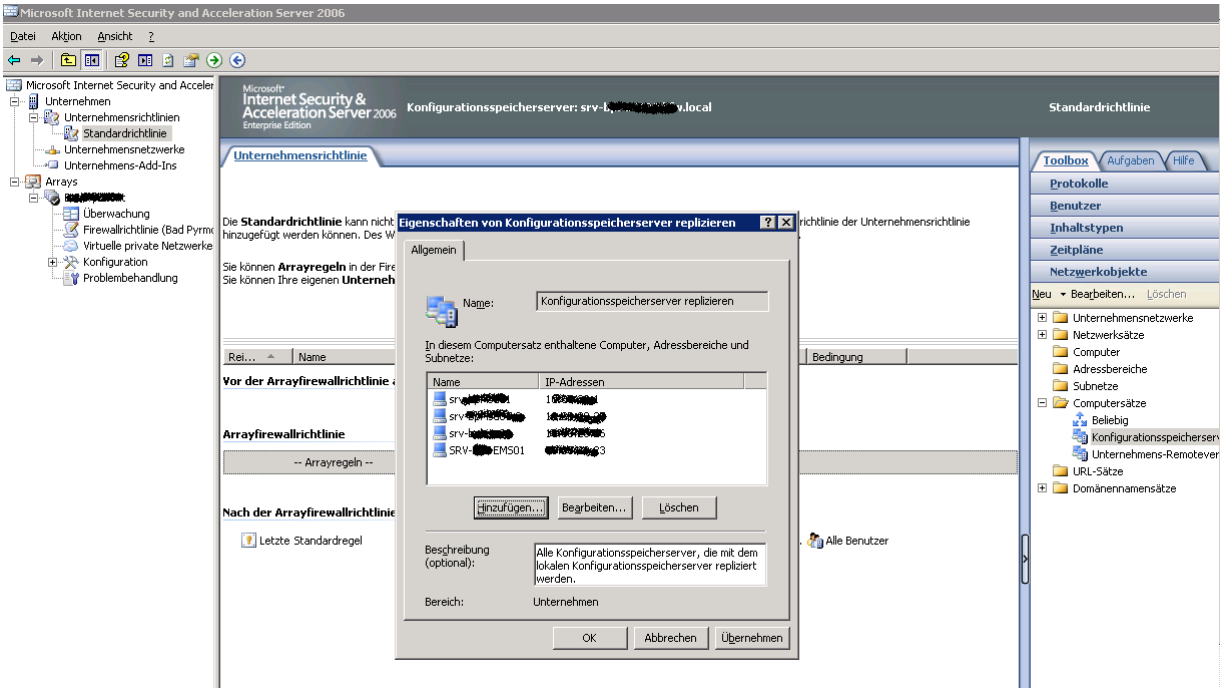
EMS installieren



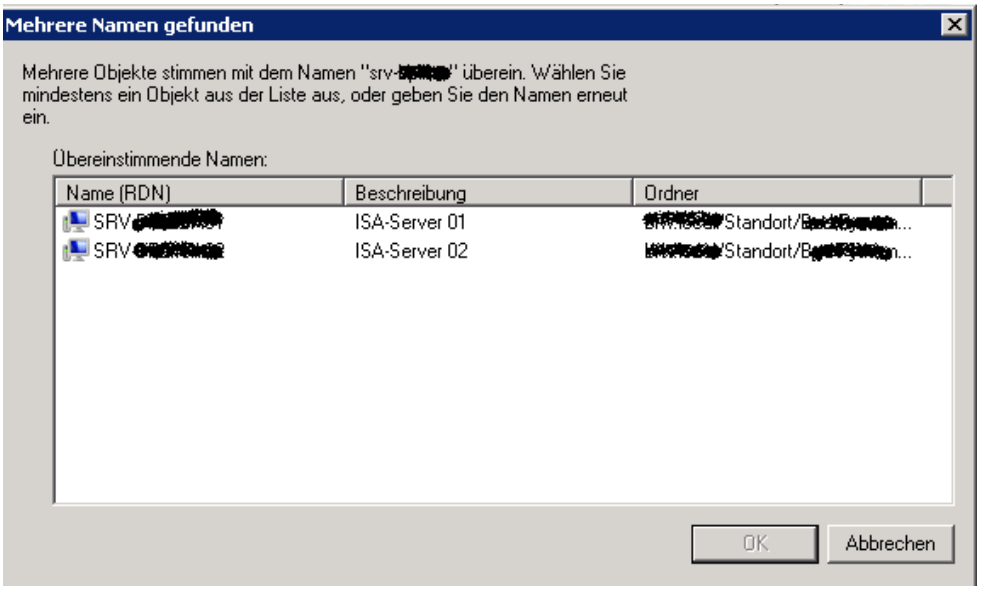
Vorhandes Unternehmen kopieren oder neu erstellen – Neu erstellen auswaehlen und die ISA Server 2006 EE Konfiguration exportieren. Bei dem Beittrit zu einem existierenden Unternehmen wird die Umgebung im Mischmodus installiert. Hier sind zusaetzliche Schritte erforderlich.



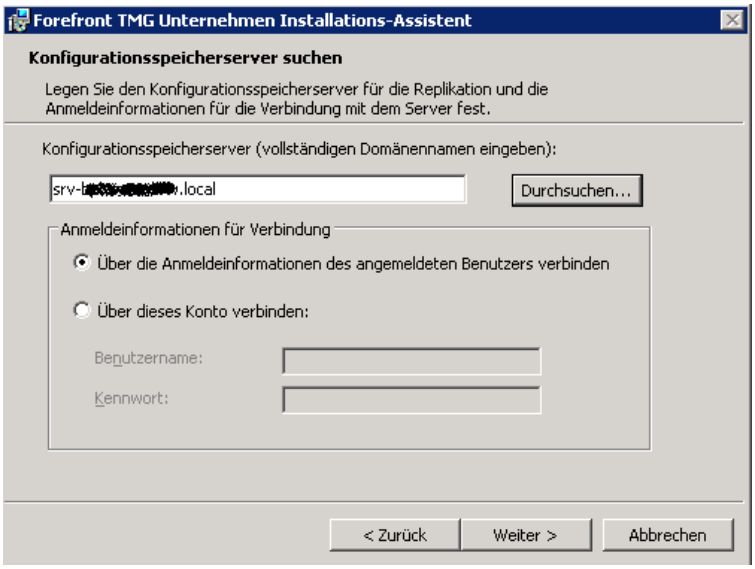
Konfigurationsspeicherserver replizieren, damit der EMS Zugriff hat



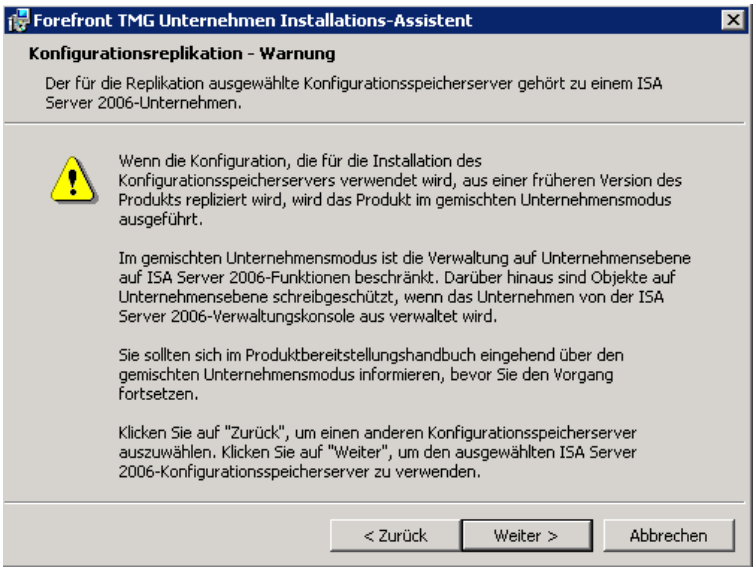
Angabe des CSS



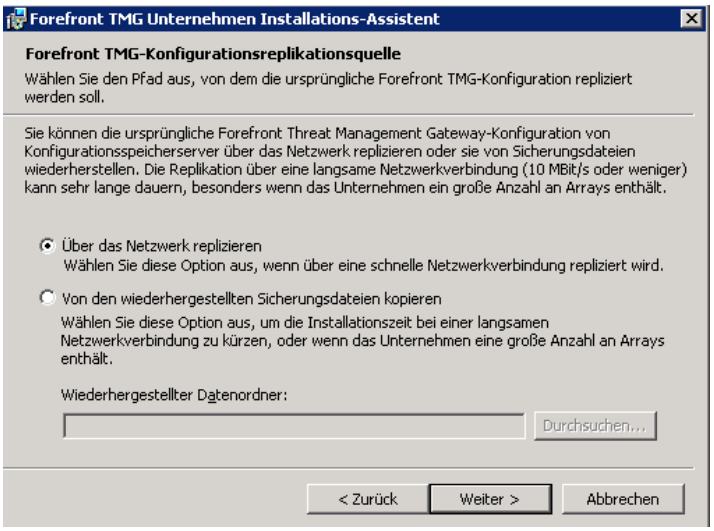
Suchen des Konfigurationsspeicherservers



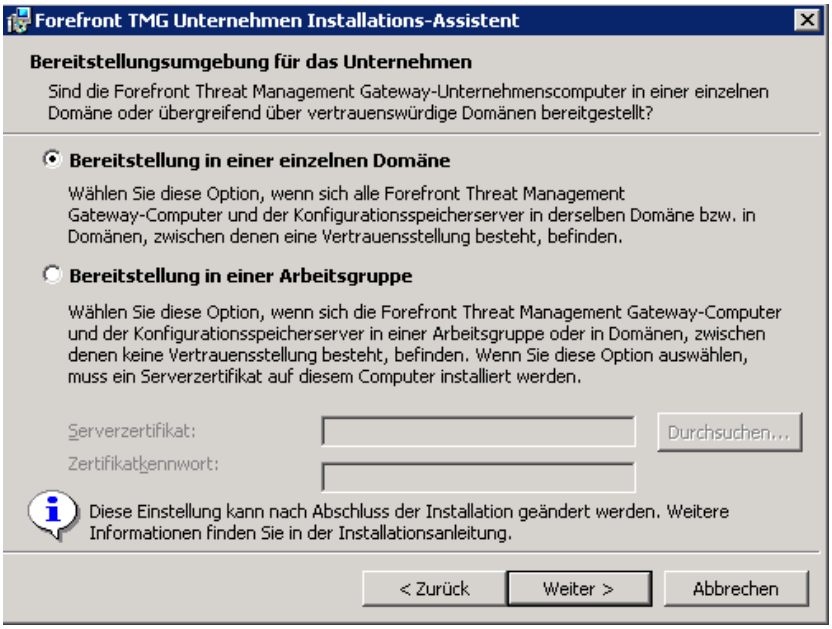
ACHTUNG:



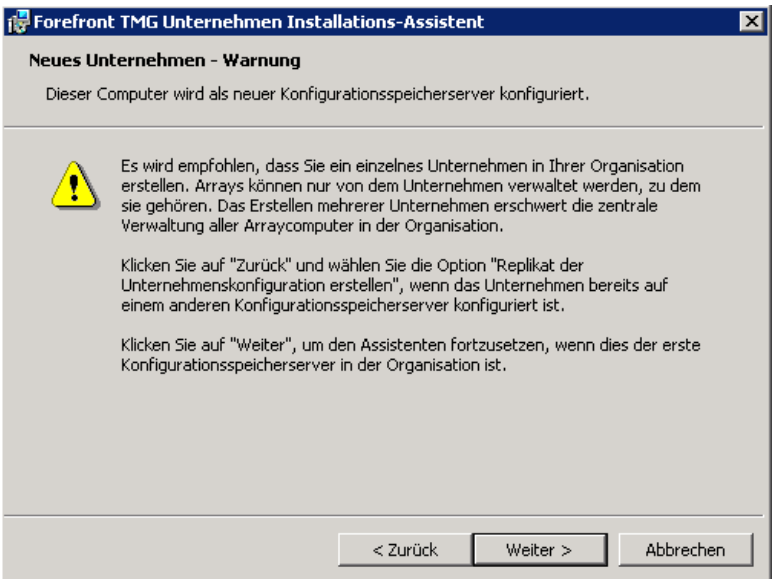
Ueber das Netzwerk replizieren



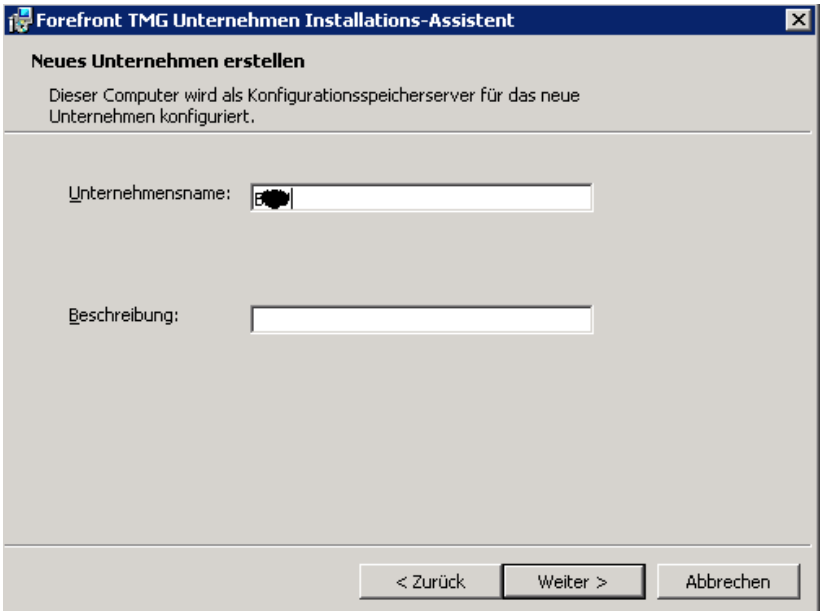
Bereitstellung in einer einzelnen Domaene



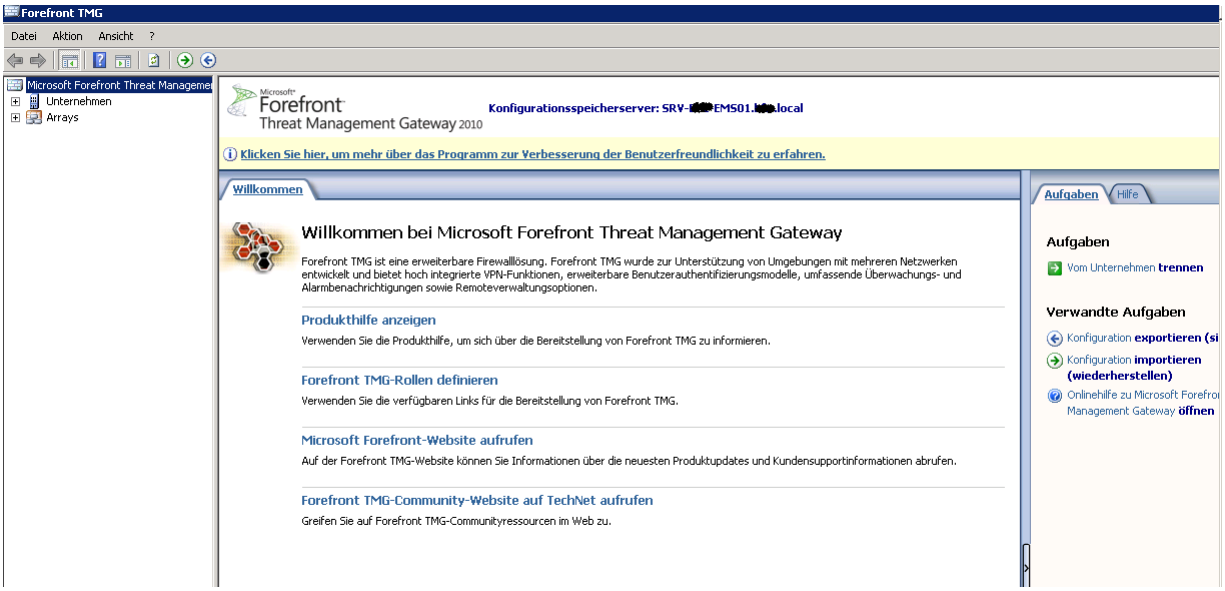
Hinweis, dass keine multiplen Forefront TMG Unternehmen erstellt werden sollten



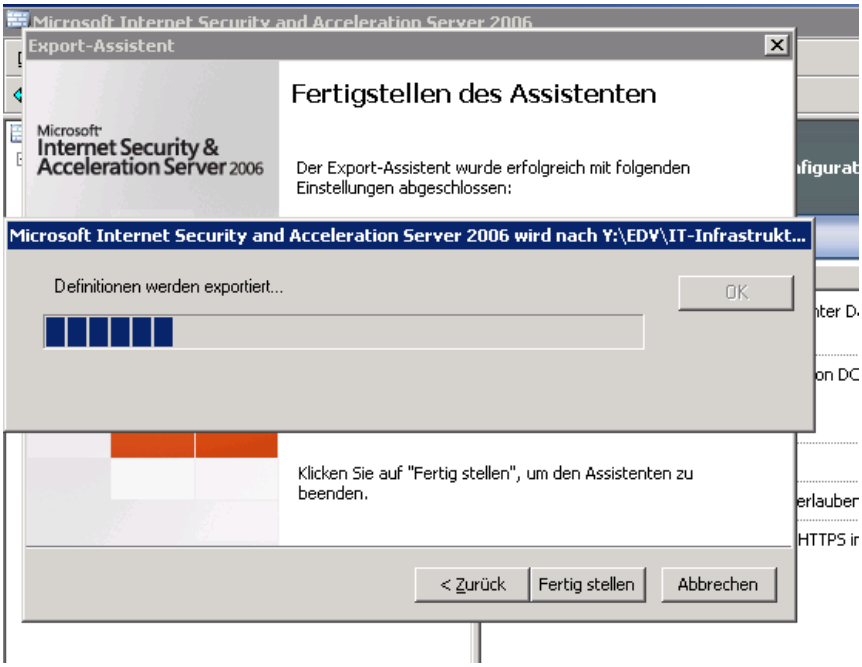
TMG Enterprise neu erstellen



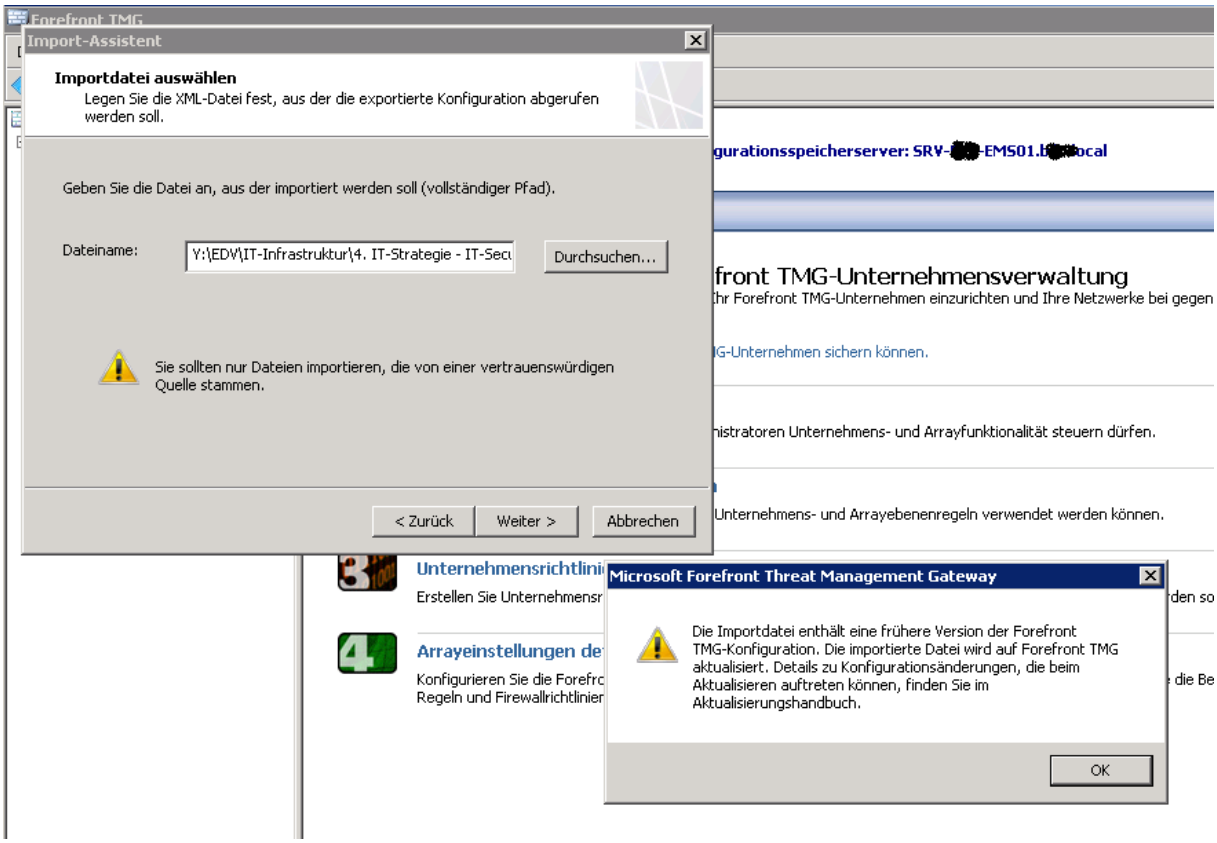
Danach kann die TMG-Verwaltungskonsole gestartet werden



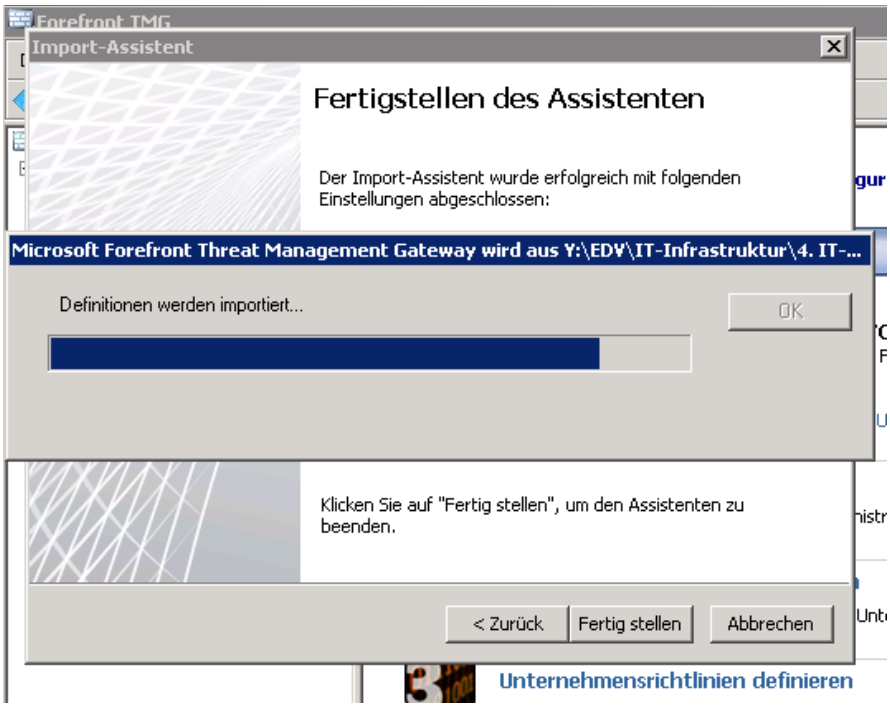
Export der ISA Server 2006 Konfiguration



Import der ISA Konfiguration in den EMS

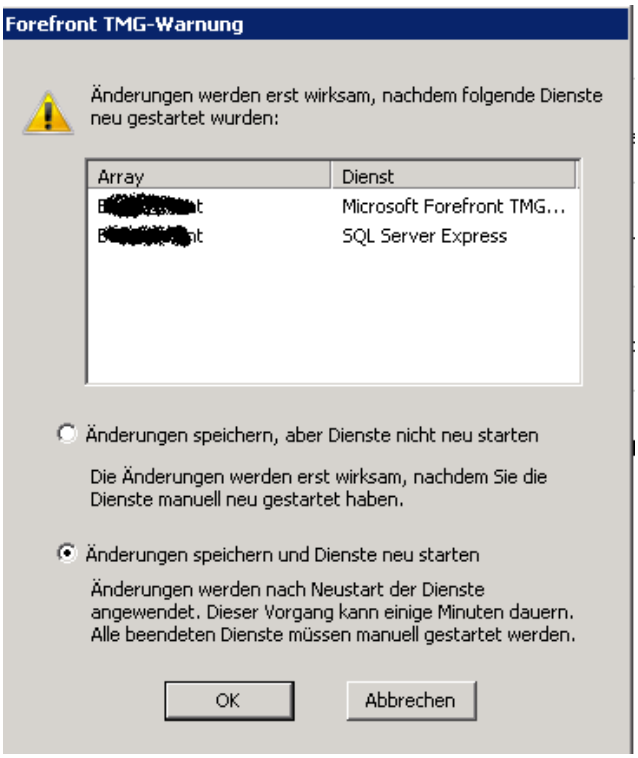


Konfig wird importiert

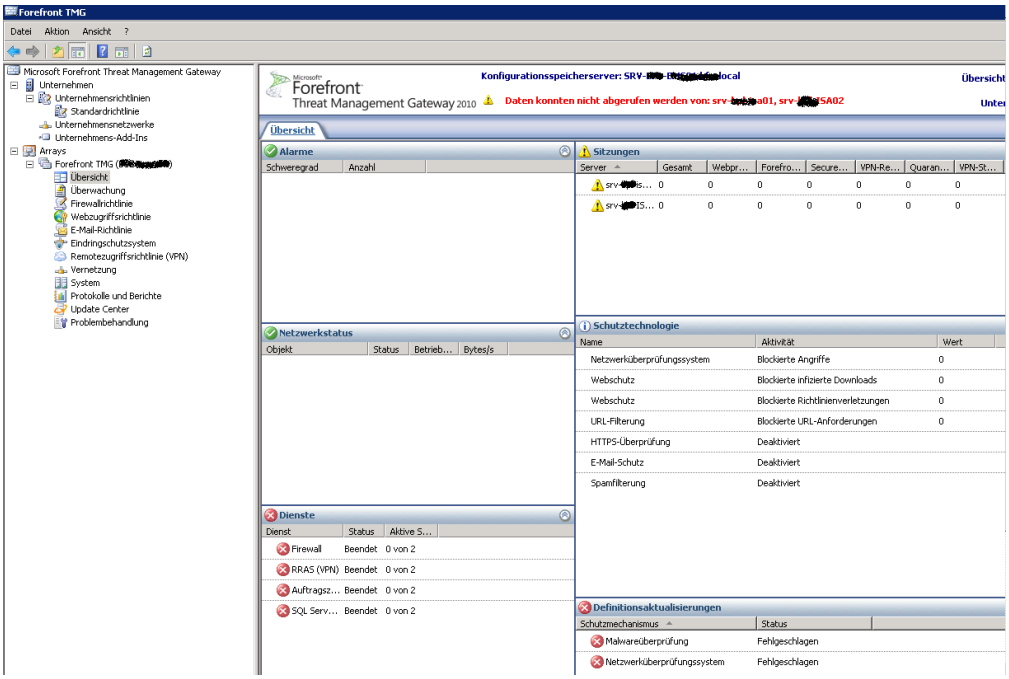


Etwas Nacharbeit ist erforderlich

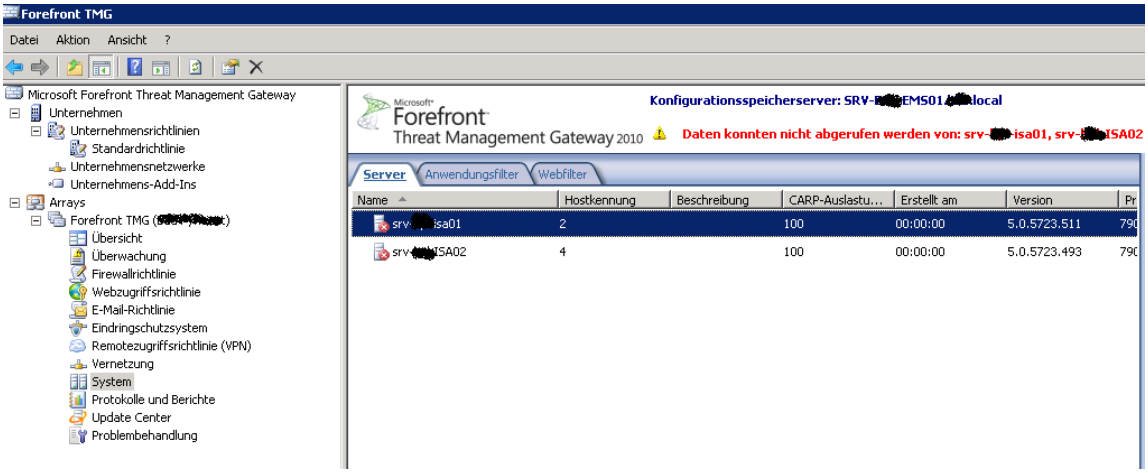
Konfigurationsaenderungen uebernehmen und Dienste neu starten

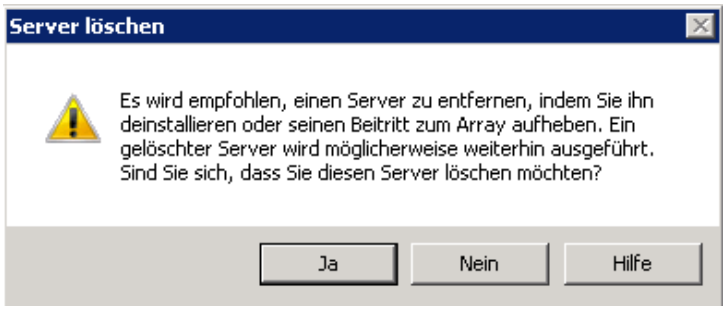


OK, die Server gibt es ja so nicht mehr im Array

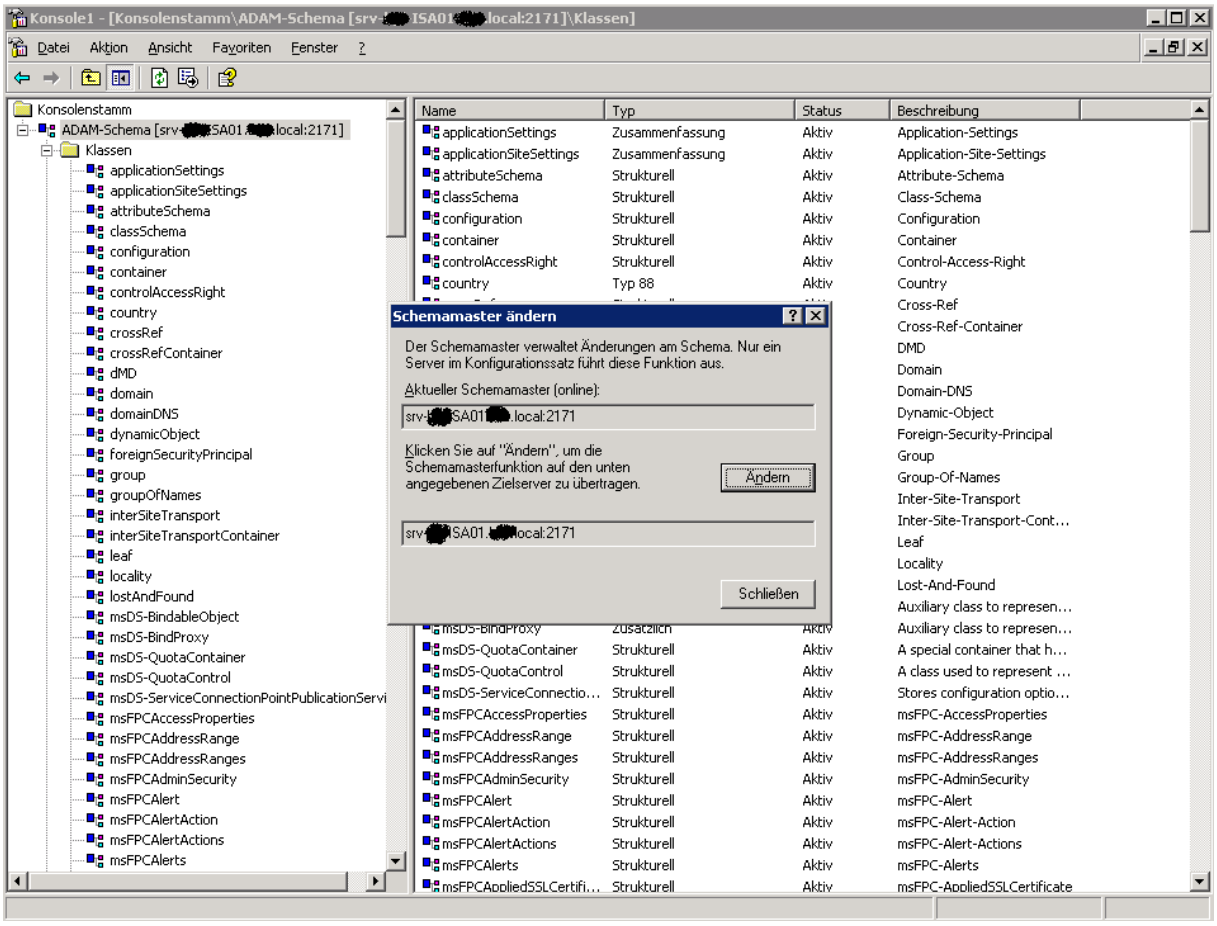


Server loeschen, da diese neu installiert werden und auch neue Namen erhalten

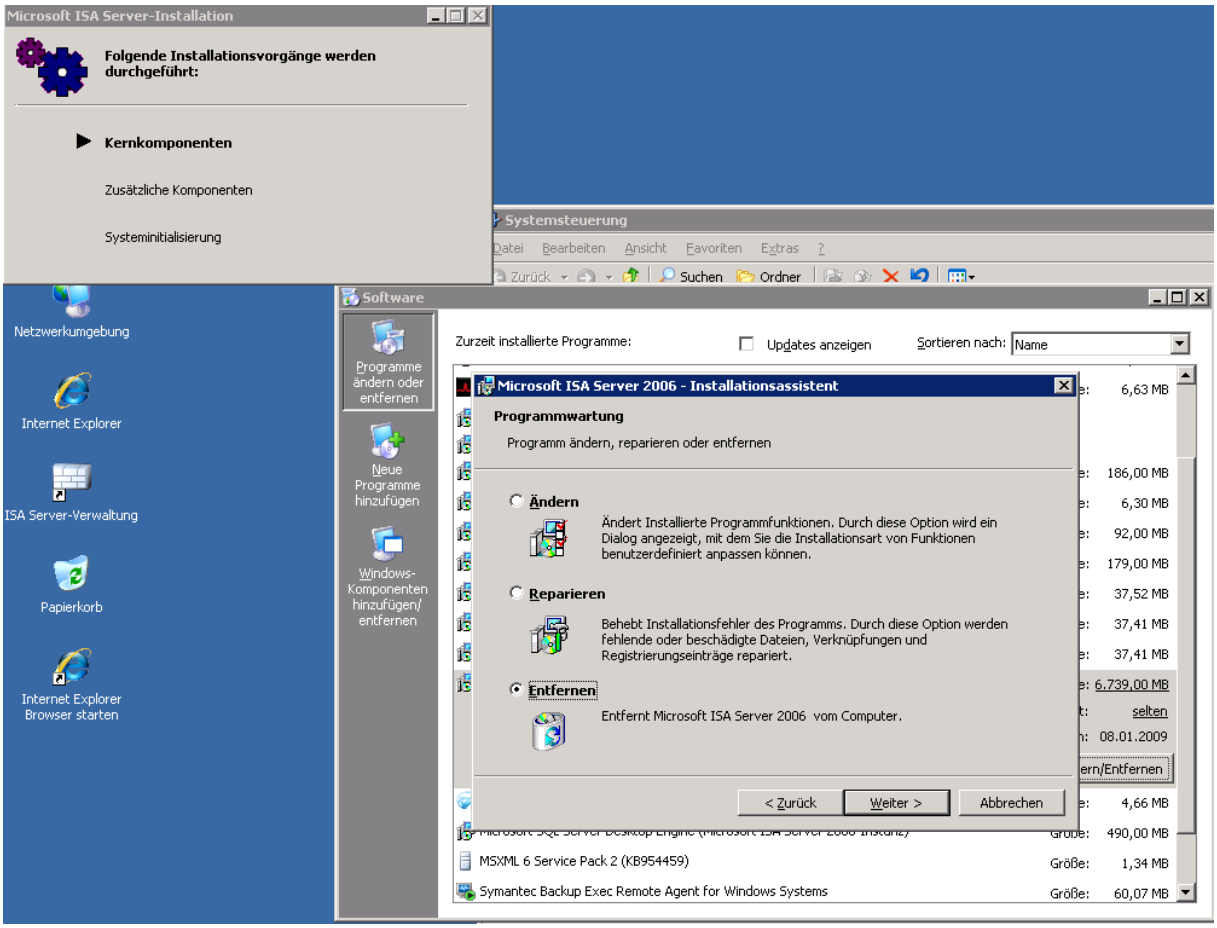




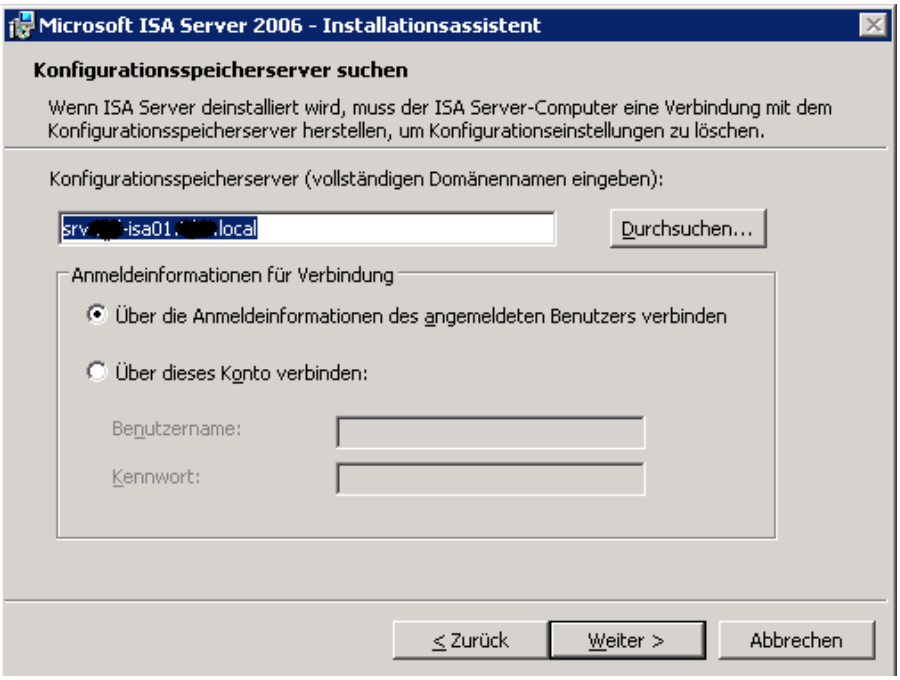
ISA Schema Master auf den Server aendern, welcher als letztes deinstalliert wird



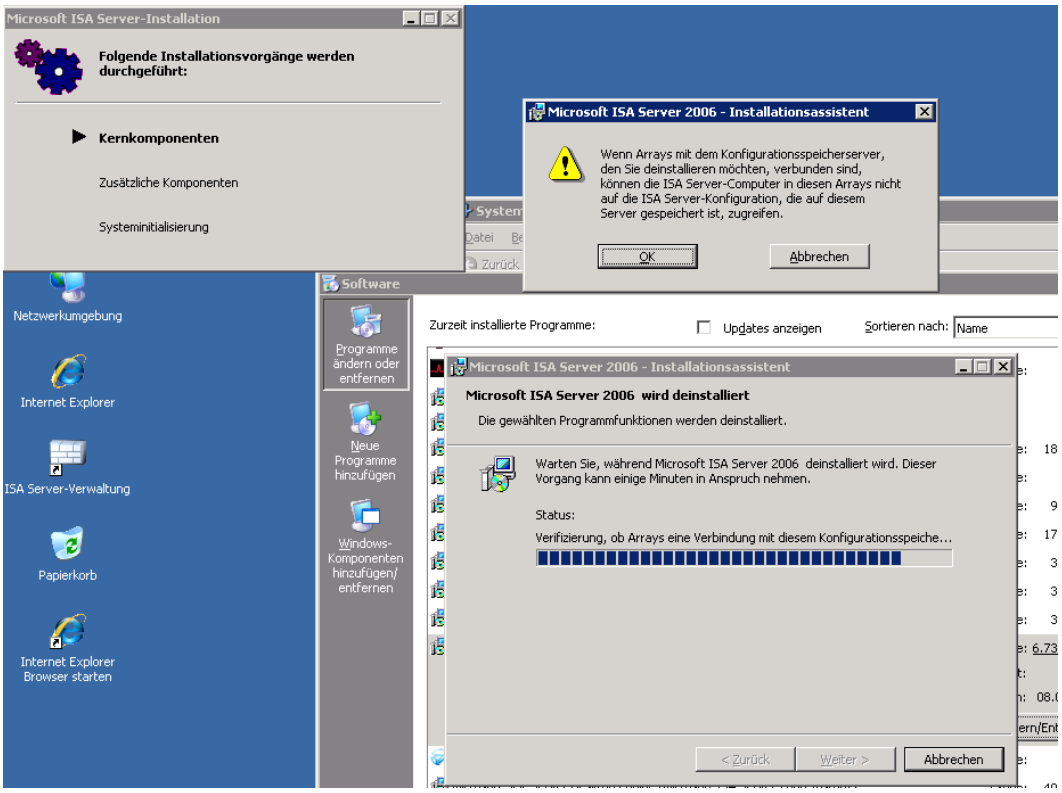
Ersten ISA Server aus dem Array deinstallieren



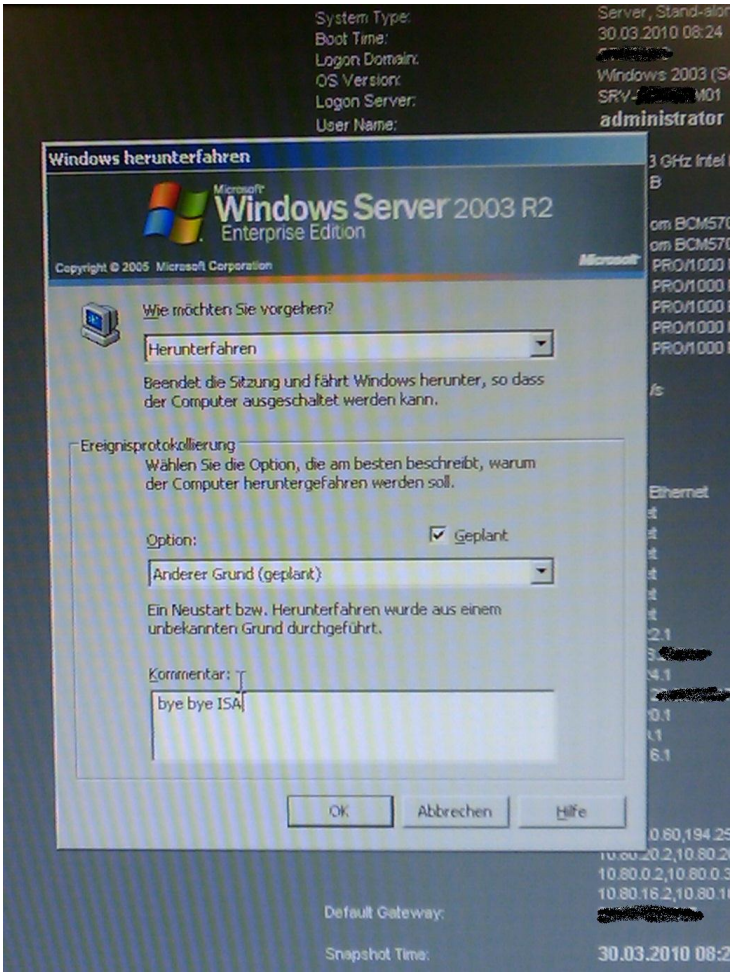
Verbindung mit CSS aufnehmen



Ja, alles weg

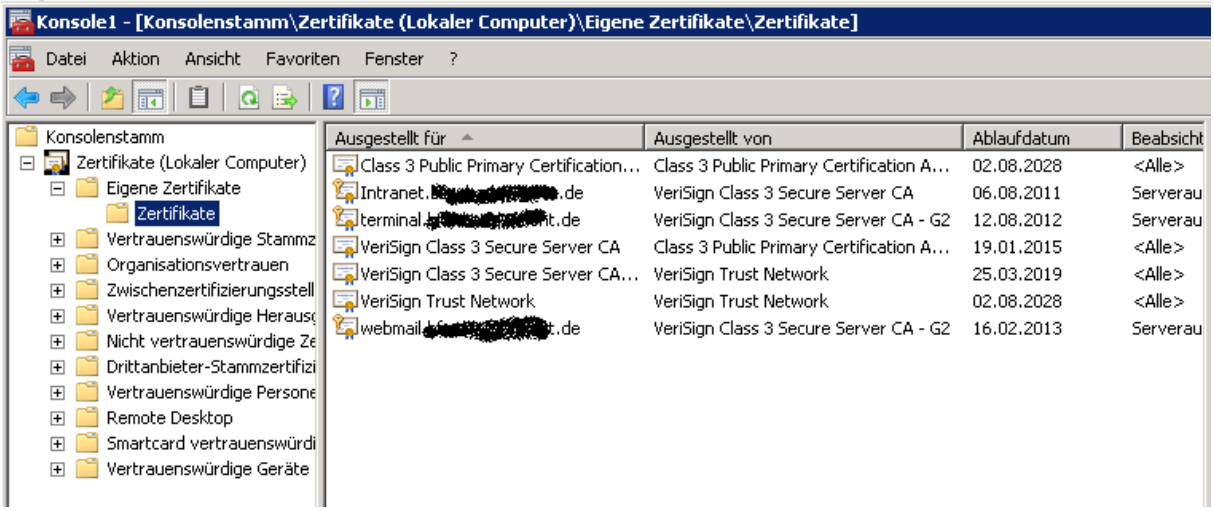


Auf Wiedersehen ☺

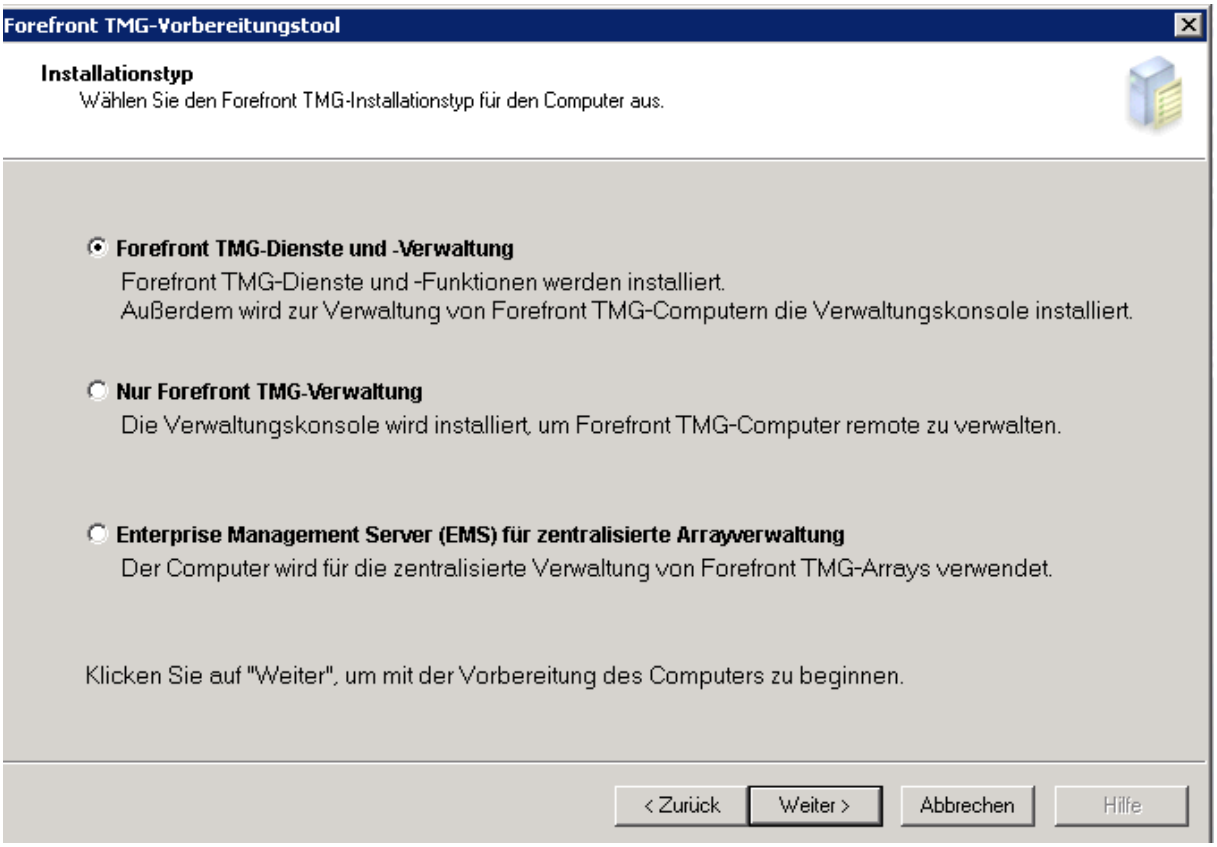


TMG Node 1 Installation

Nach der obligatorischen Windows Installation, Anpassung der Netzwerkkarten etc. Zertifikate aus ISA 2006 importieren.

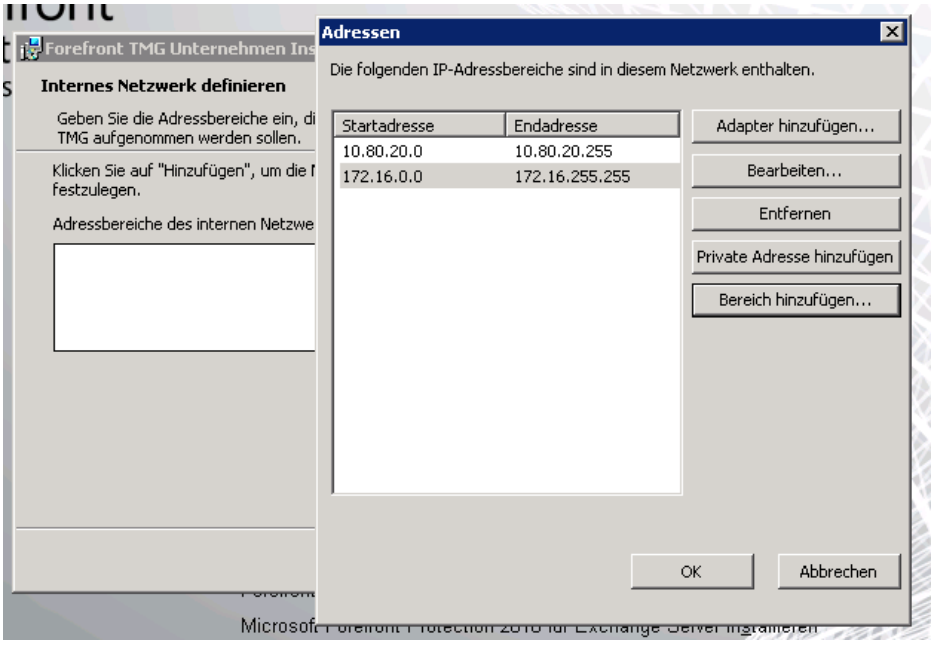


TMG Vorbereitungstool

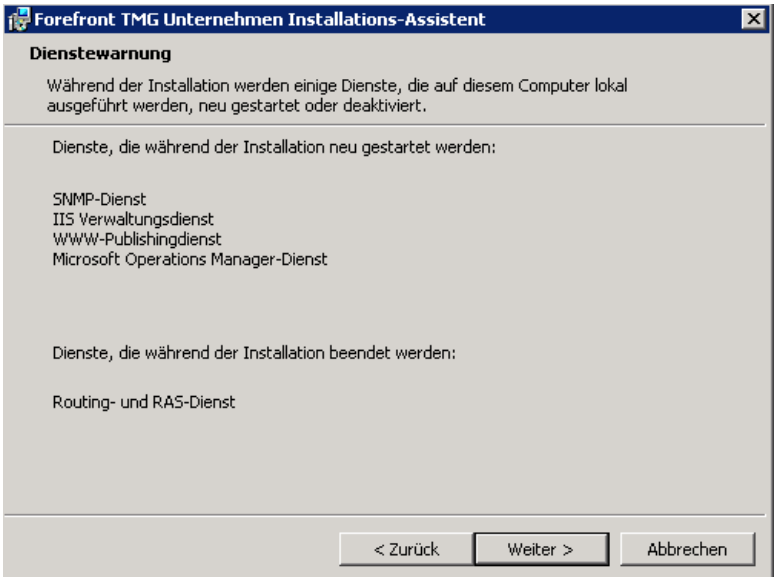


TMG installieren

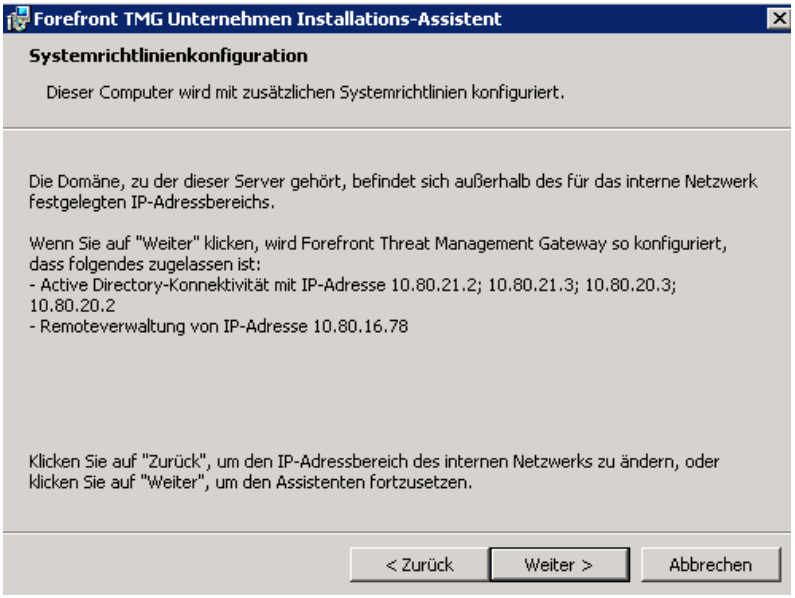
Interne IP-Adressbereiche angeben



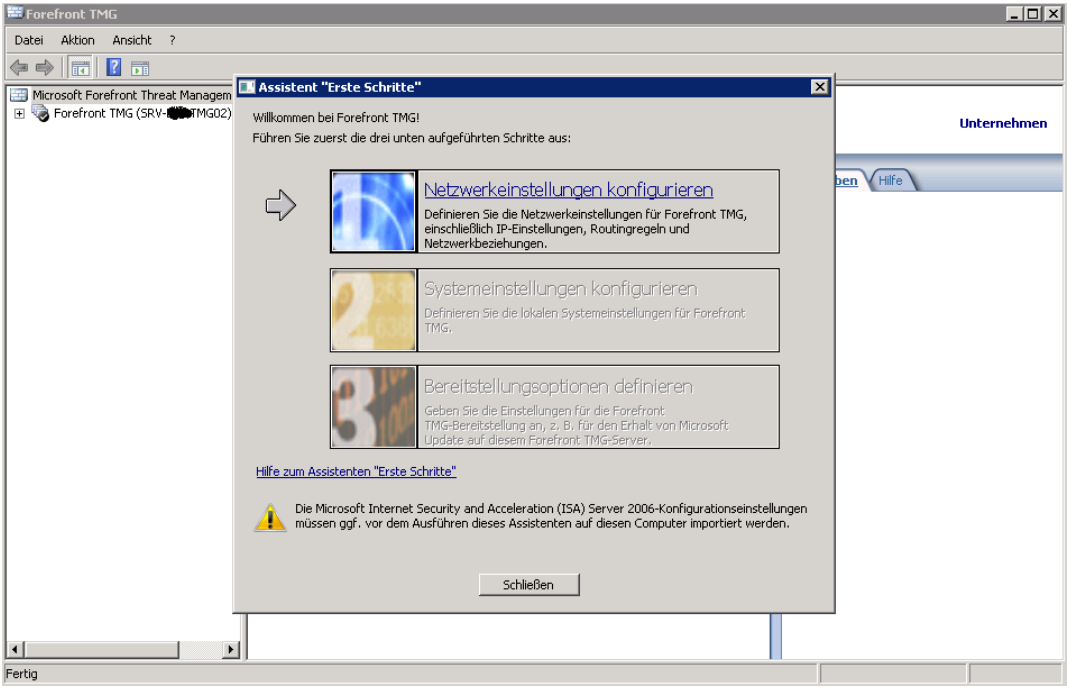
Waehrend der Installation zu beendende Dienste, so sie denn installiert sind



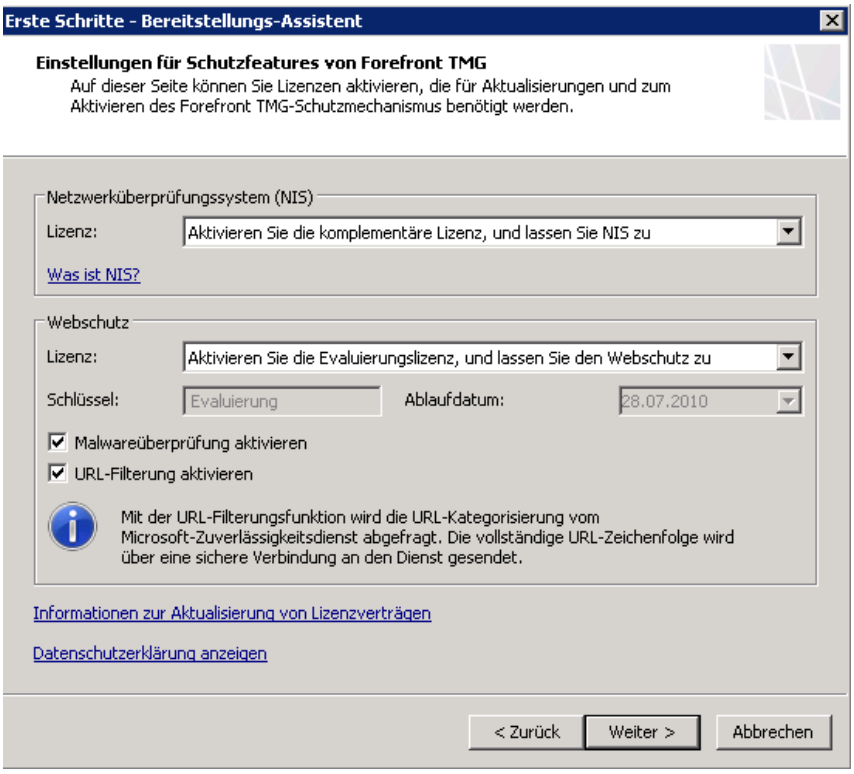
Systemrichtlinienkonfiguration fuer AD-Zugriff und Remoteverwaltung (spaeter anpassen)



Nach erfolgter Installation TMG Erstinstallationswizard ausfuehren

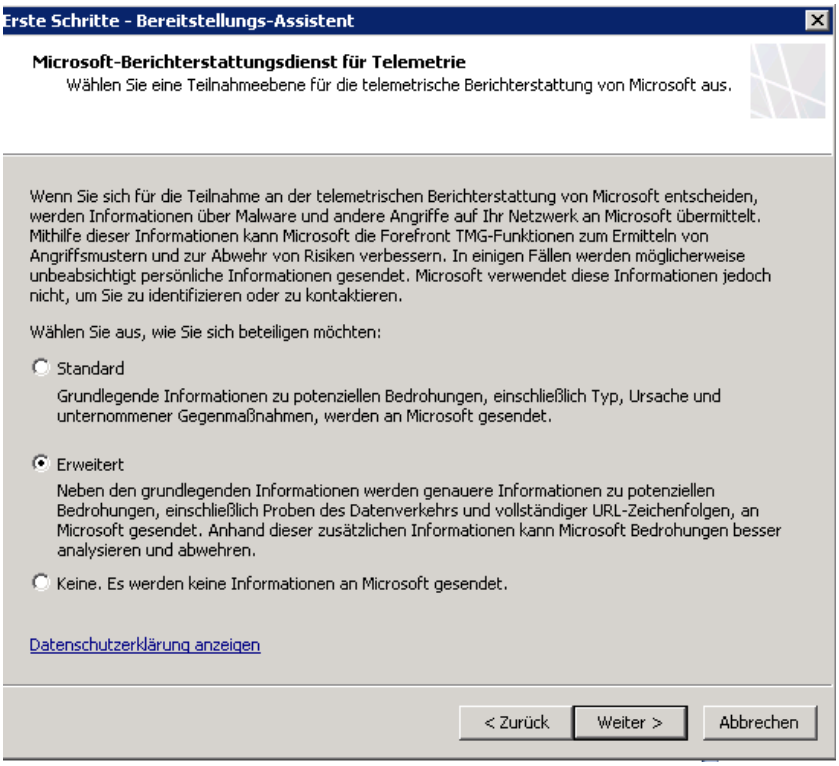


Domaenenmitglieschaft, Netzwerkkartenkonfiguration usw.

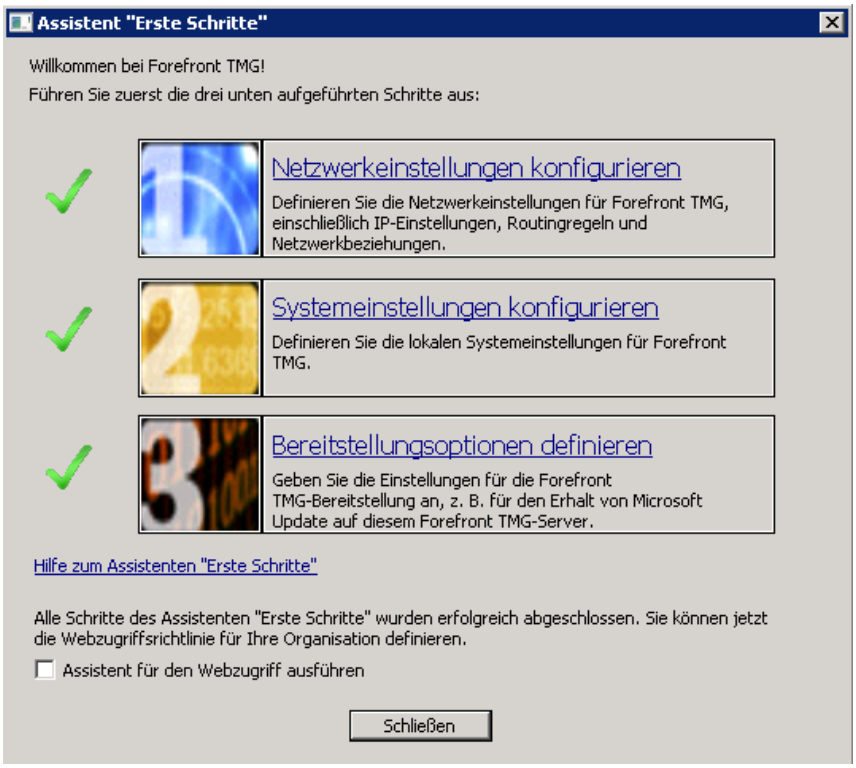


Anmerkung: Fragen Sie mal einen grossen Softwardistributor nach den Lizenzen fuer die WPS, Sie koennten ueberrascht werden, dass der Distributor keine Ahnung hat, woher die Lizenzen kommen, geschweige denn, was das fuer Lizenzen sind ☹

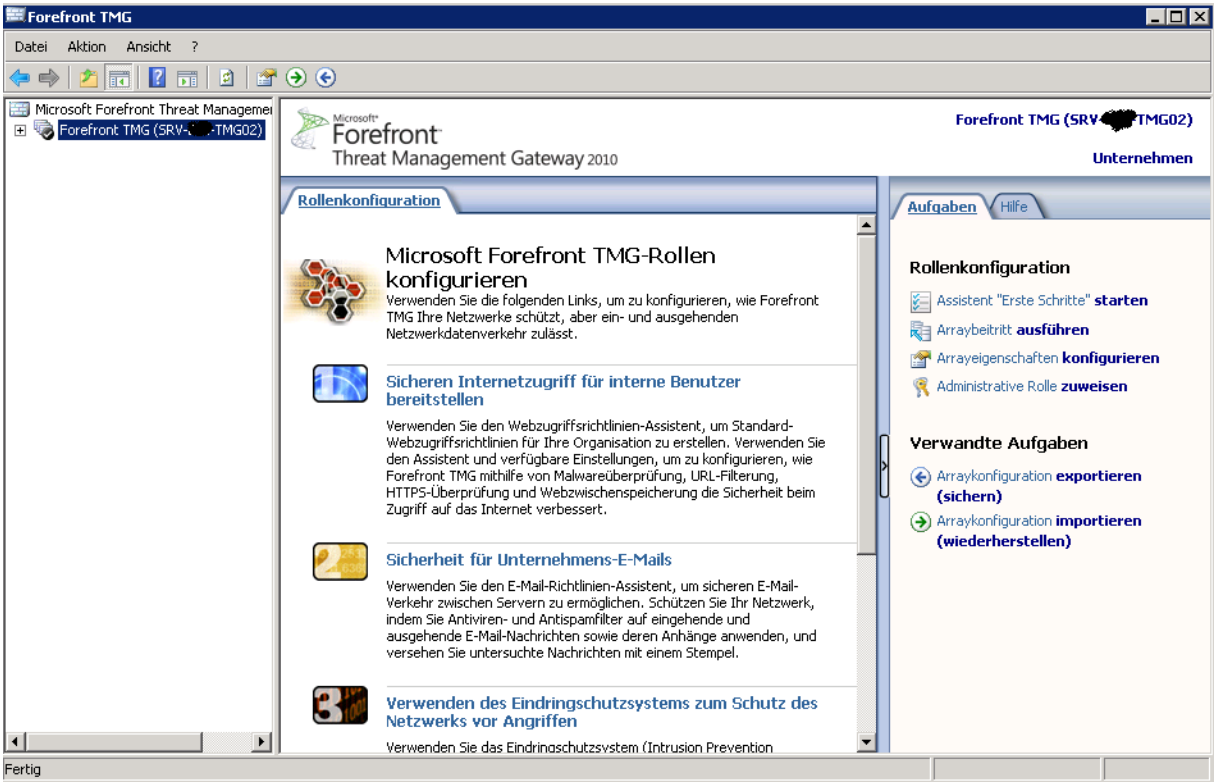
Erweiterte Telemetrie waehlen wegen NIS/Malware etc.



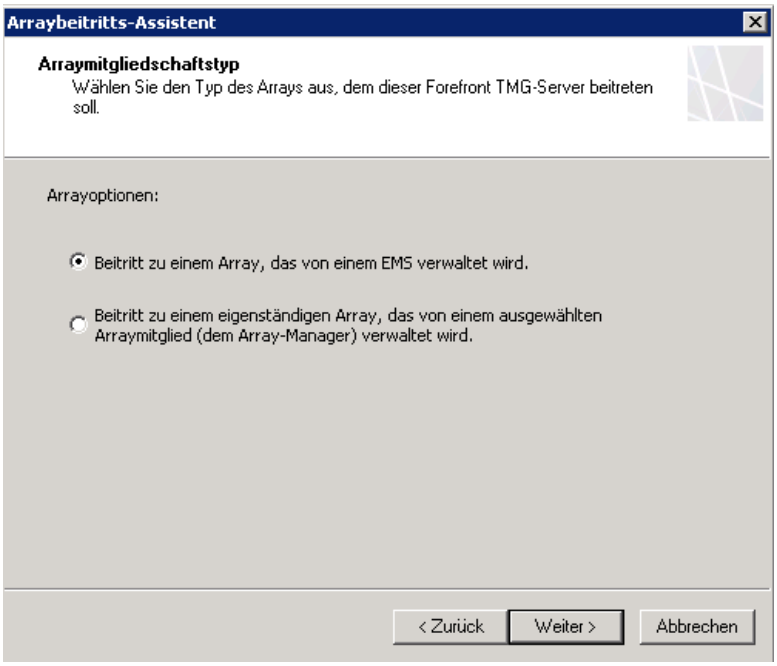
Assistenten fuer Webzugriff nicht ausfuehren



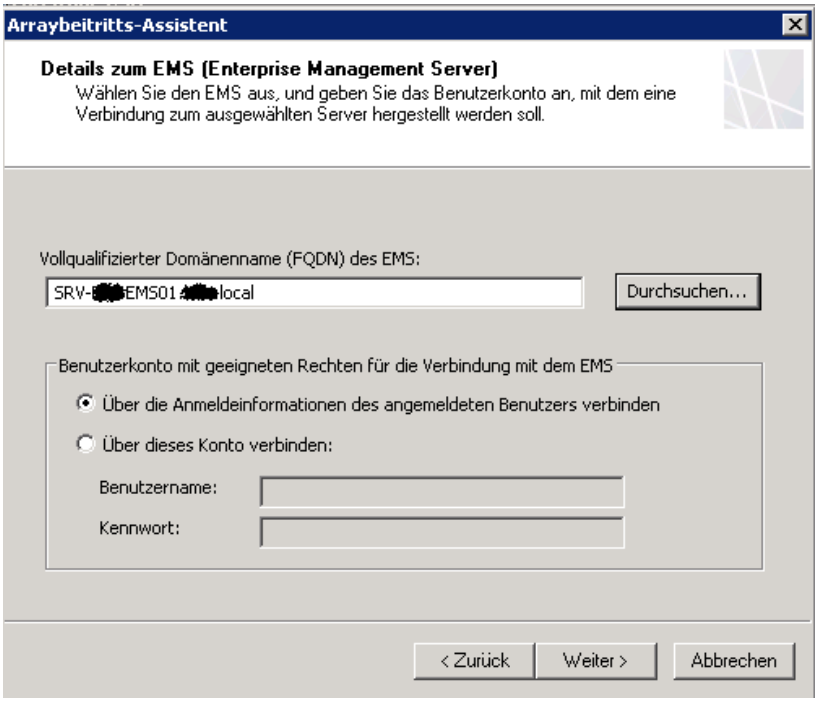
Arraybeitritt ausfuehren



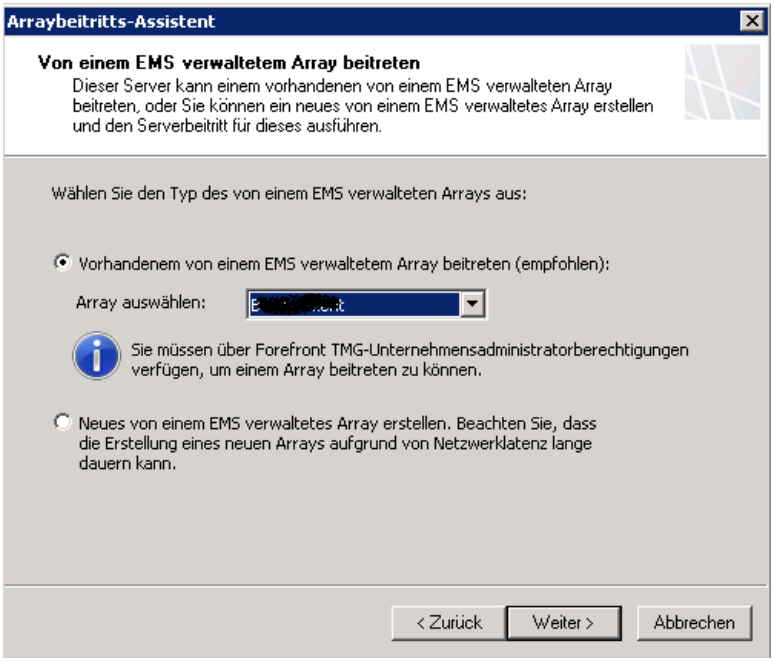
EMS Beitritt



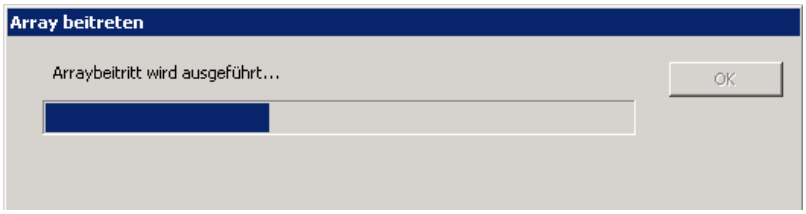
EMS Server angeben



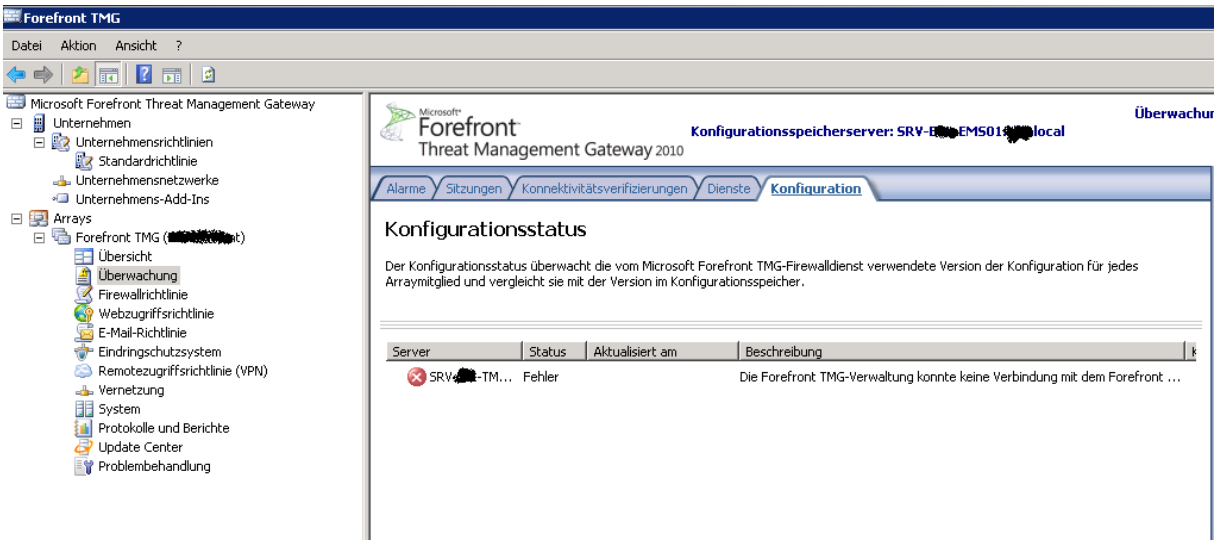
EMS Array waehlen



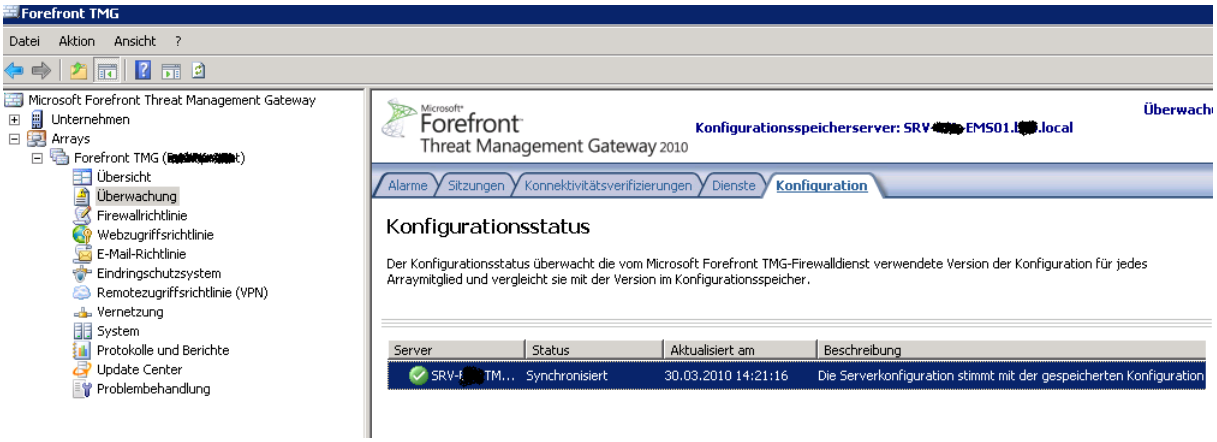
Ab geht es



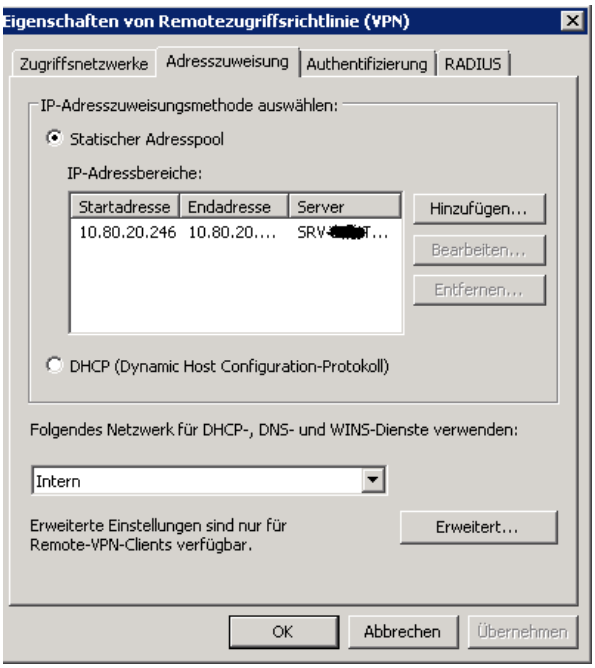
Da taucht schon was auf dem EMS auf



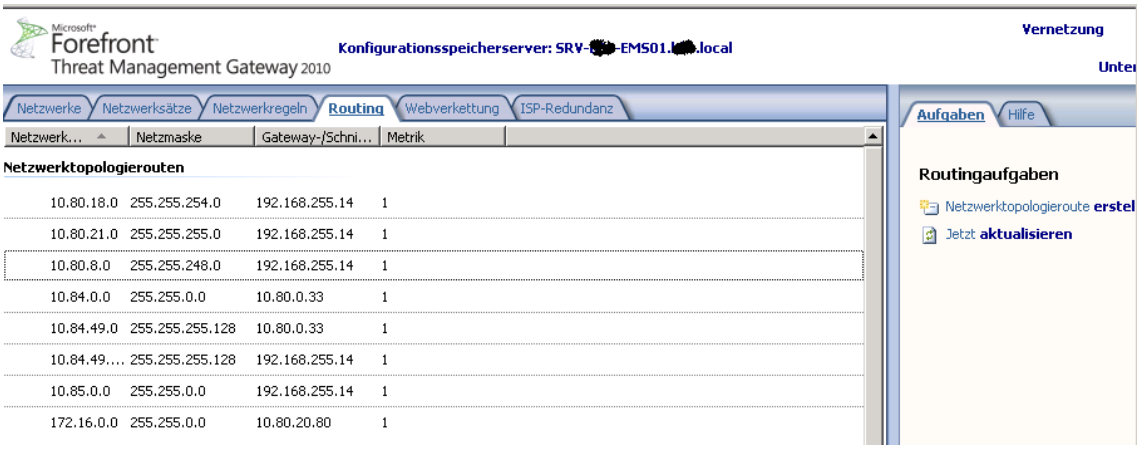
Alles schoen. Dauert etwas?!



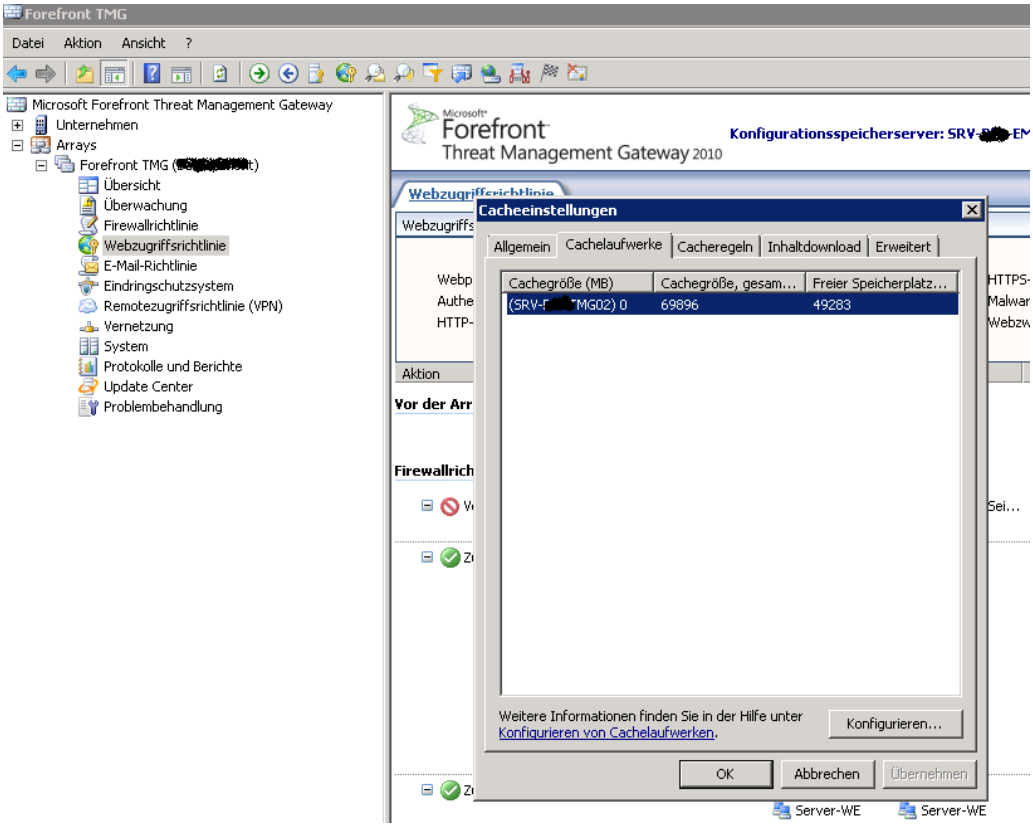
VPN Konfiguration



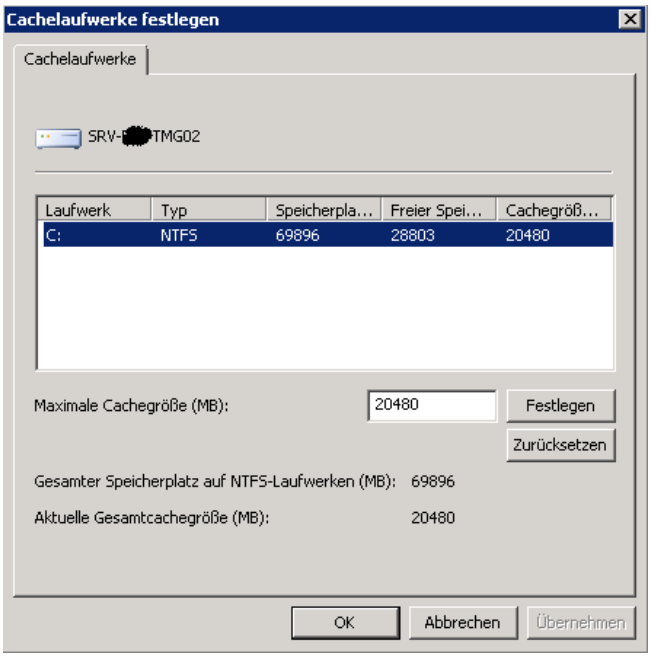
Routen adden – jetzt sehr schoen im EMS gespeichert und ueber die GUI konfigurierbar.



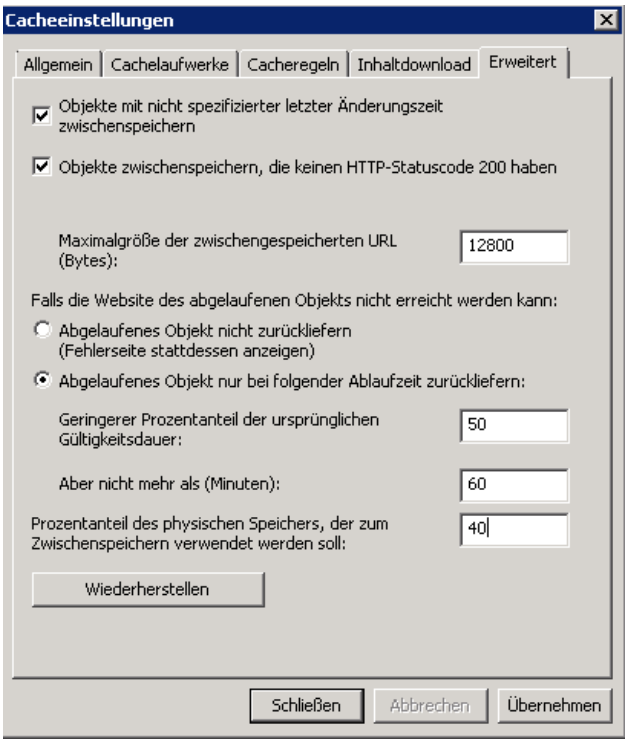
Cache Konfiguration



Cachegroesse festlegen



Cachesize auf 40% vergroessern

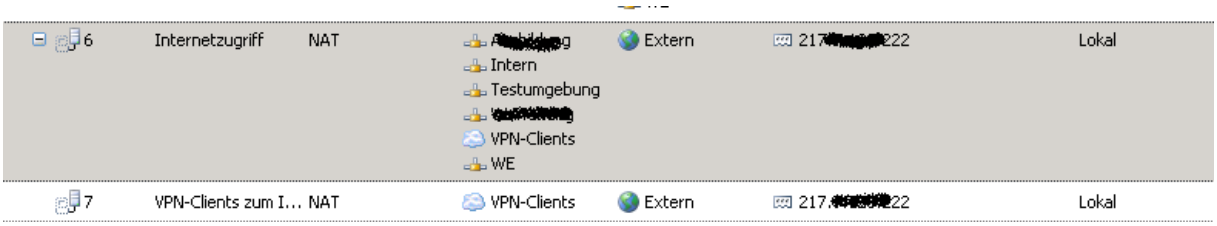


Konfigurationsaenderung uebernehmen und Dienste neu starten

Nach den vorgenommenen Aenderungen kann der TMG Server in Produktionsbetrieb genommen werden und die Funktionaliaet eingehend getestet werden.

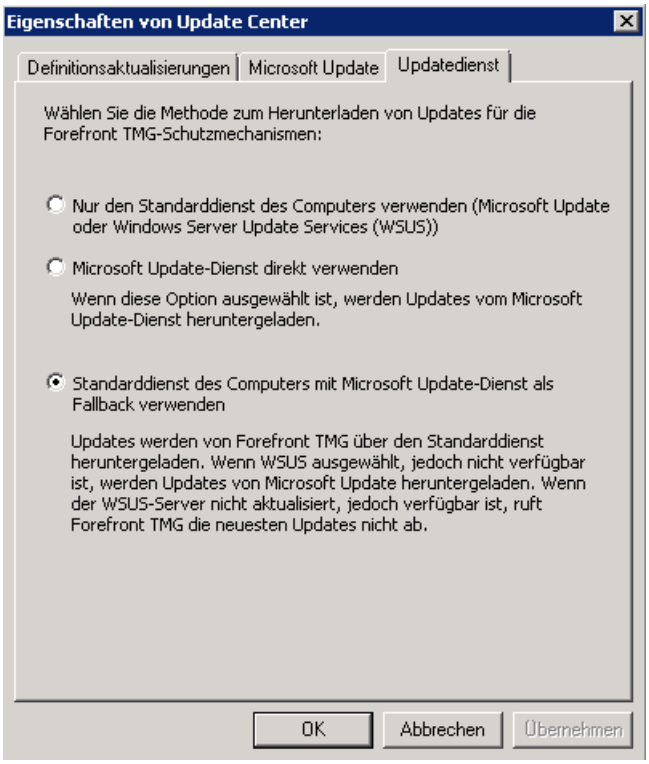
ACHTUNG:

Wenn mehrere IP-Adressen an das externe Netzwerkinterface gebunden sind und auf der vorliegenden Firewall nur Verbindungen auf einer bestimmten IP-Adresse angenommen werden, scheint TMG nicht mehr die erste gebundene IP-Adresse am Netzwerkinterface zu verwenden, so dass man in der TMG Konfiguration die ausgehende IP-Adresse angeben muss:

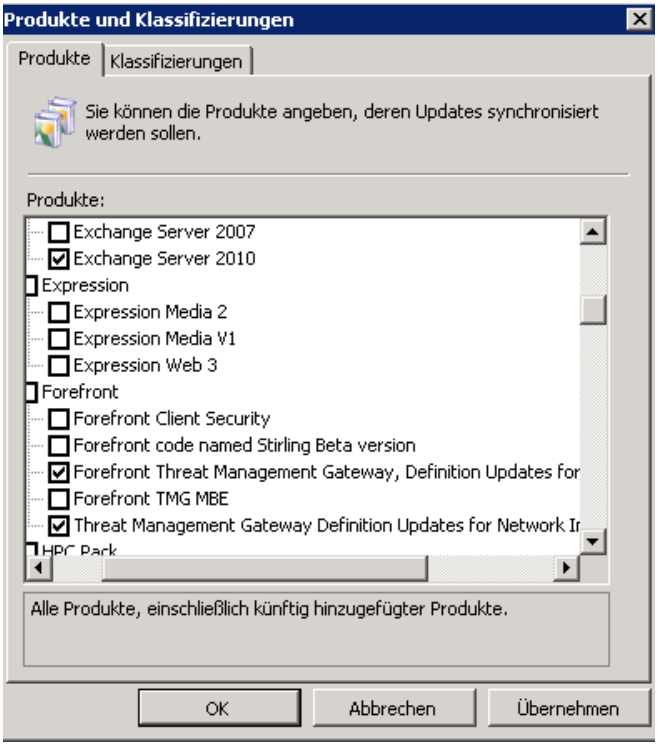


Das scheint bei Design so zu sein und kein TMG Problem:
http://support.microsoft.com/kb/969029/en-us - Danke an Jason Jones fuer die Info.
http://social.technet.microsoft.com/Forums/en-US/ForefrontedgePub/thread/52b08c5d-6652-4d79-8f46-f9125905d73d/

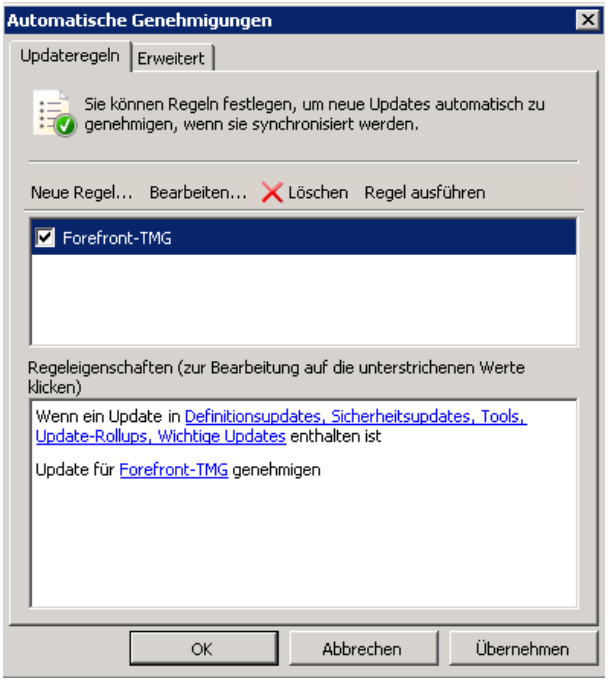
WSUS fuer Updates verwenden



WSUS fuer TMG Updates konfigurieren



Automatische Genehmigungsregel fuer TMG



WSUS Updateintervall auf 12x am Tag stellen

Gruppenrichtlinie fuer WSUS fuer die TMG Server zur automatischen Installation einrichten

WSUS Automatisch fuer Forefront TMG

Daten ermittelt am: 31.03.2010 08:53:28

Computerkonfiguration (Aktiviert)

Richtlinien

Administrative Vorlagen

Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher abgerufen.

Windows-Komponenten/Windows Update

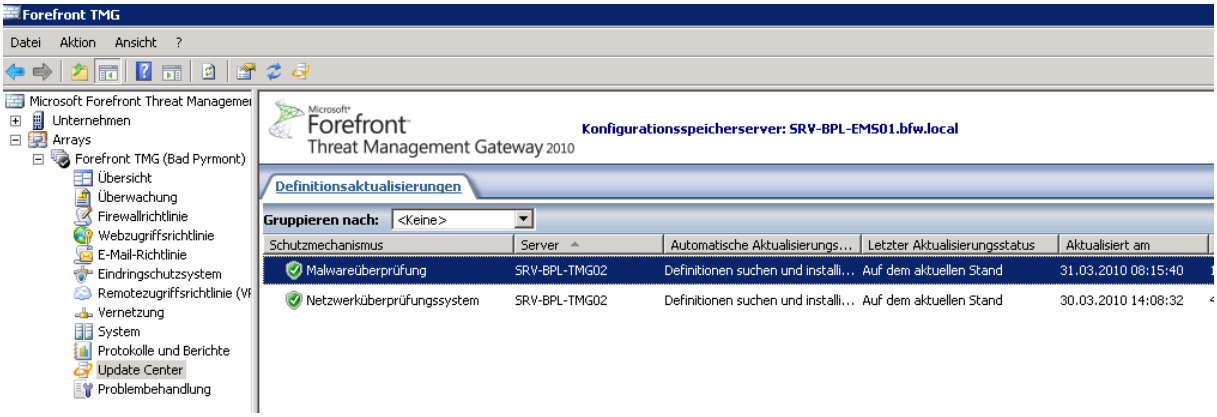
Richtlinie	Einstellung	Kommentar
Automatische Updates konfigurieren	Aktiviert	
Automatische Updates konfigurieren: Folgende Einstellungen sind nur erforderlich und gültig, wenn 4 ausgewählt wird.	4 - Autom. Herunterladen und laut Zeitplan installieren	
Geplanter Installationstag:	0 - Täglich	
Geplante Installationszeit:	03:00	

Richtlinie	Einstellung	Kommentar
Automatische Updates sofort installieren	Aktiviert	
Clientseitige Zielzuordnung aktivieren	Aktiviert	
Zielgruppenname für diesen Computer	Forefront-TMG	

Richtlinie	Einstellung	Kommentar
Empfohlene Updates über automatische Updates aktivieren	Aktiviert	
Internen Pfad für den Microsoft Updatedienst angeben	Aktiviert	
Interner Updatedienst zum Ermitteln von Updates:	http://srv-b[redacted]dom01.b[redacted]local	
Intranetserver für die Statistik: (Beispiel: http://IntranetUpd01)	http://srv-b[redacted]dom01.b[redacted]local	

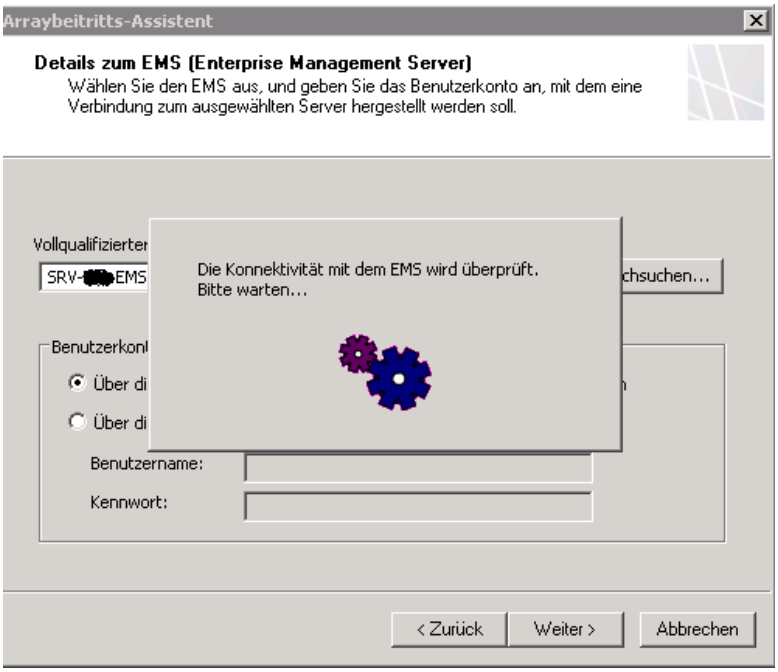
Richtlinie	Einstellung	Kommentar
Keinen automatischen Neustart für geplante Installationen durchführen	Aktiviert	
Suchhäufigkeit für automatische Updates	Aktiviert	
In folgenden Abständen (Stunden) nach Updates suchen:	2	

Updates laden

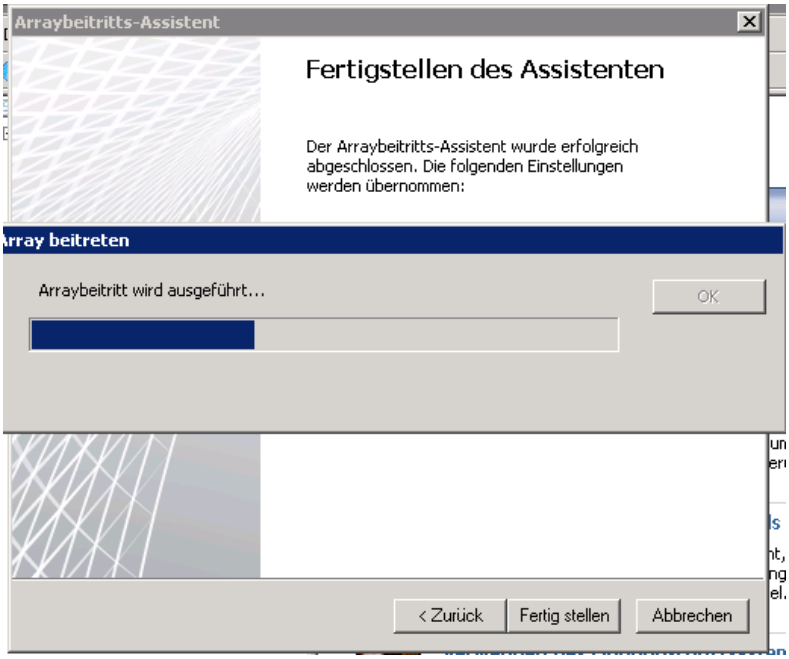


Zweiten Forefront TMG Knoten installieren

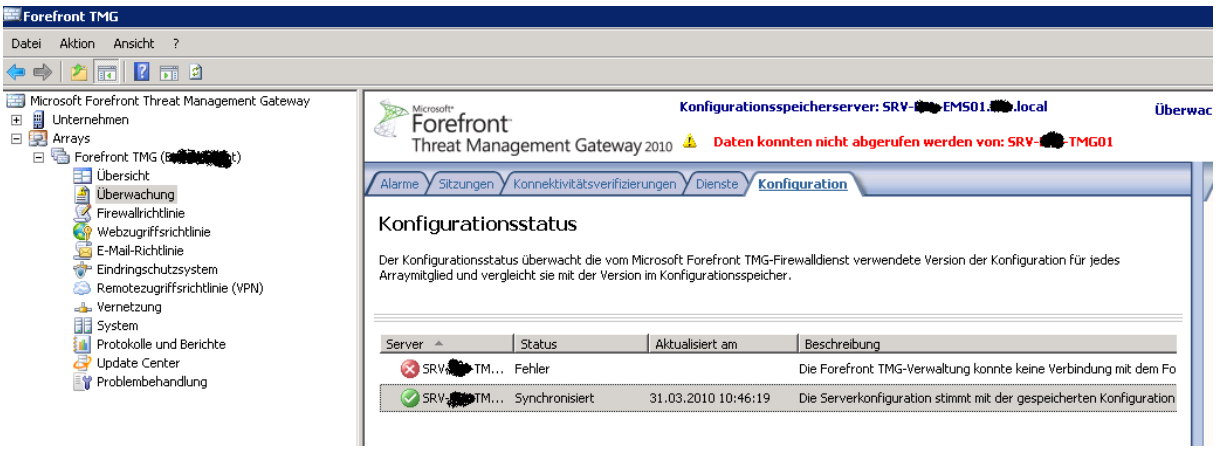
Dem EMS beitreten



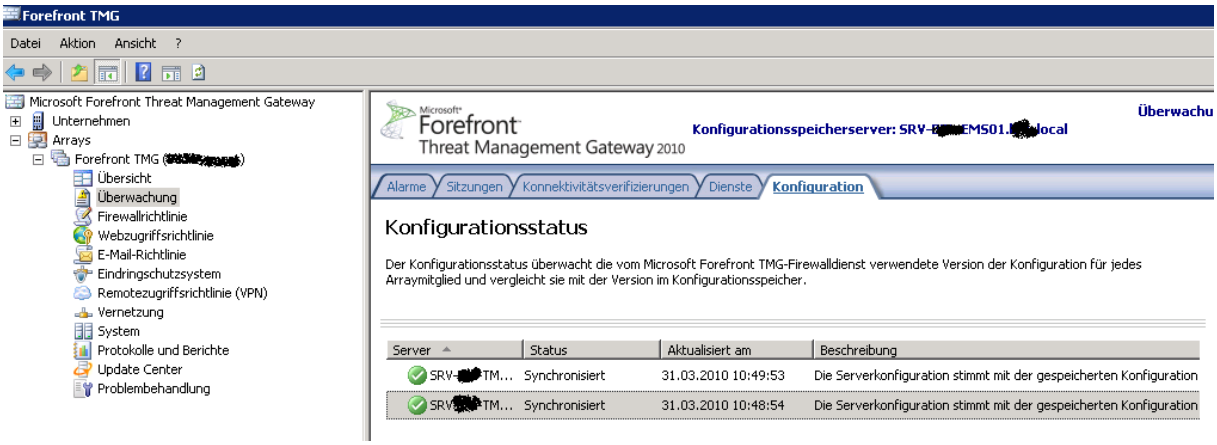
Beitritt wird durchgefuehrt



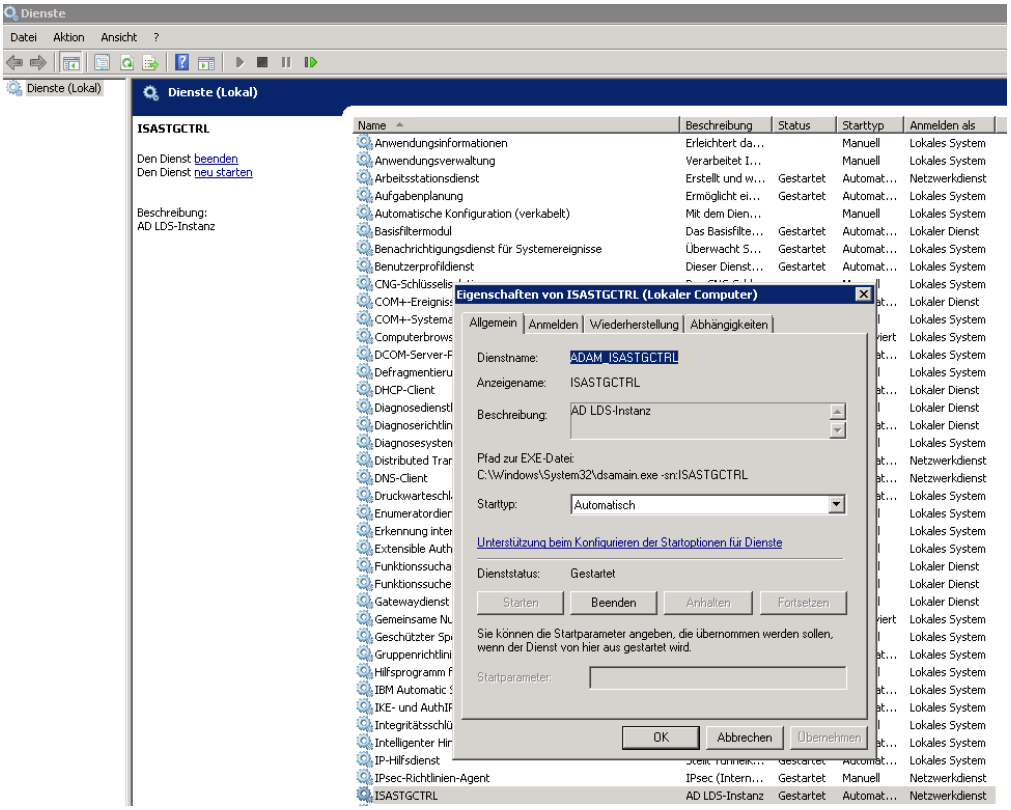
So langsam tut sich was



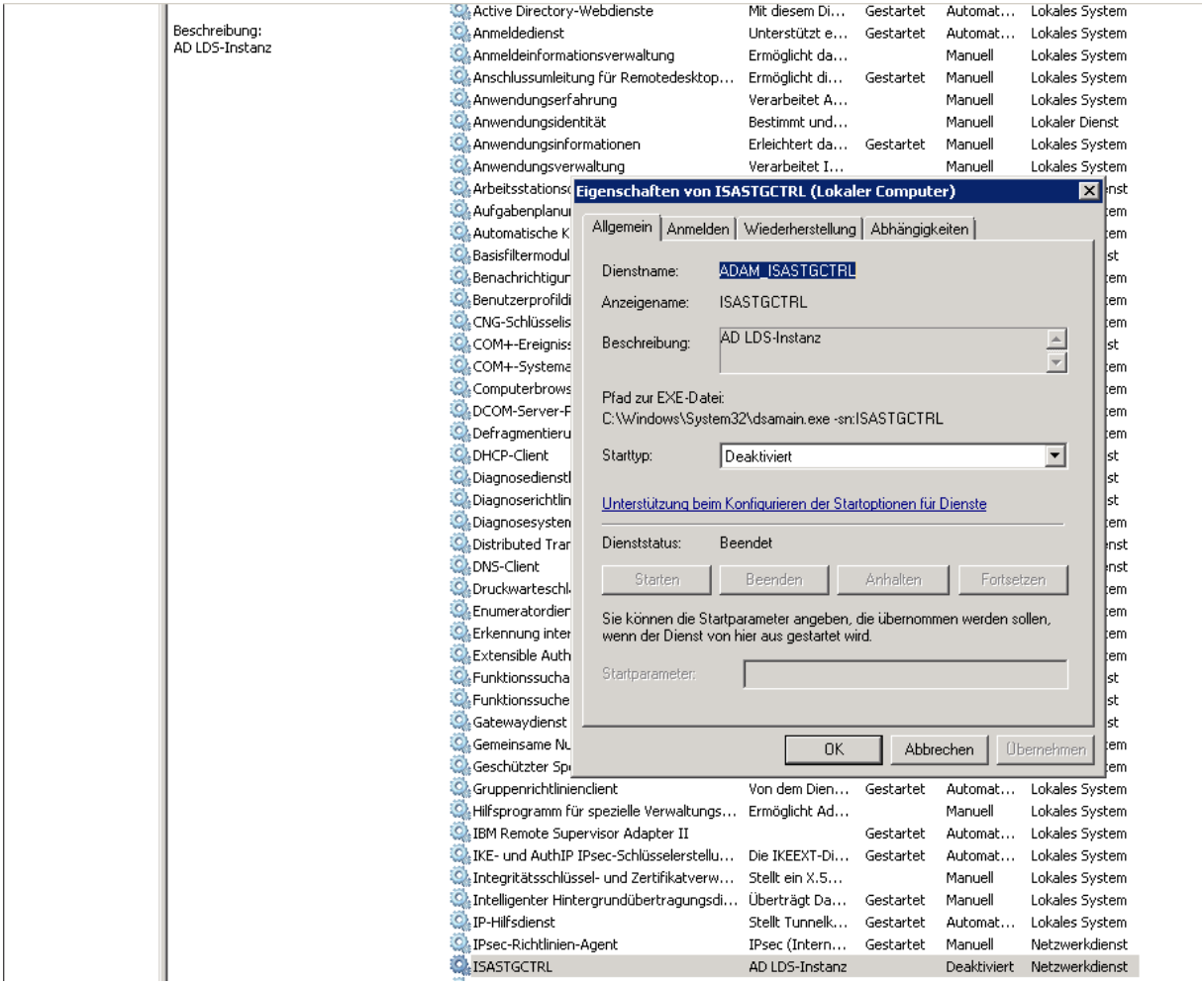
Erfolgreich



Vor Array Beitritt wird eine lokale AD-LDS Instanz genutzt

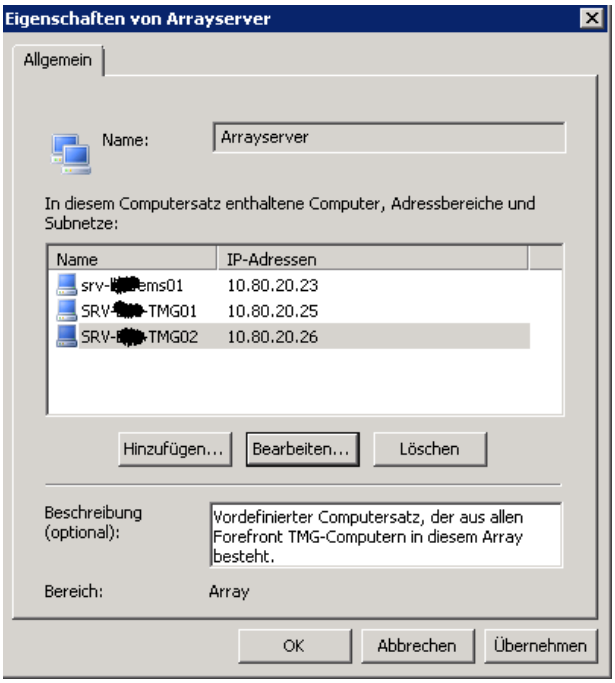


Nach Array Beitritt wird die lokale Instanz deaktiviert, da die Konfigurationsdaten vom zentralen EMS bereitgestellt werden

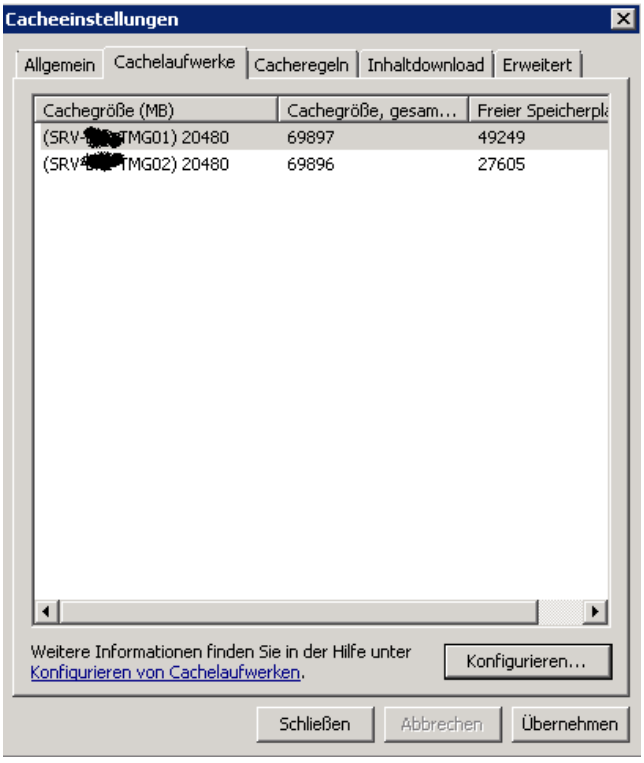


EMS anpassen fuer TMG Node Zugriff

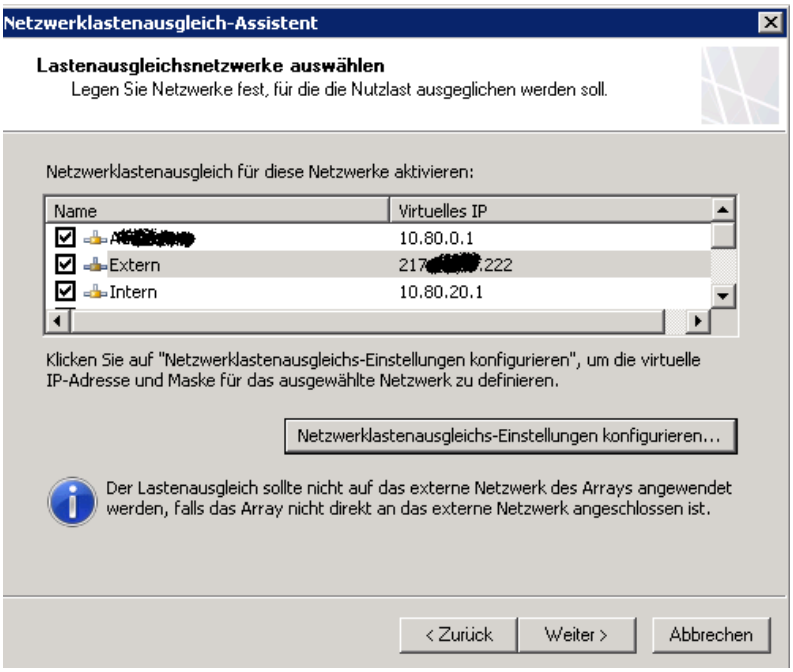
Die ISA Server Reste aus der importierten Konfiguration in den Systemrichtlinien entfernen



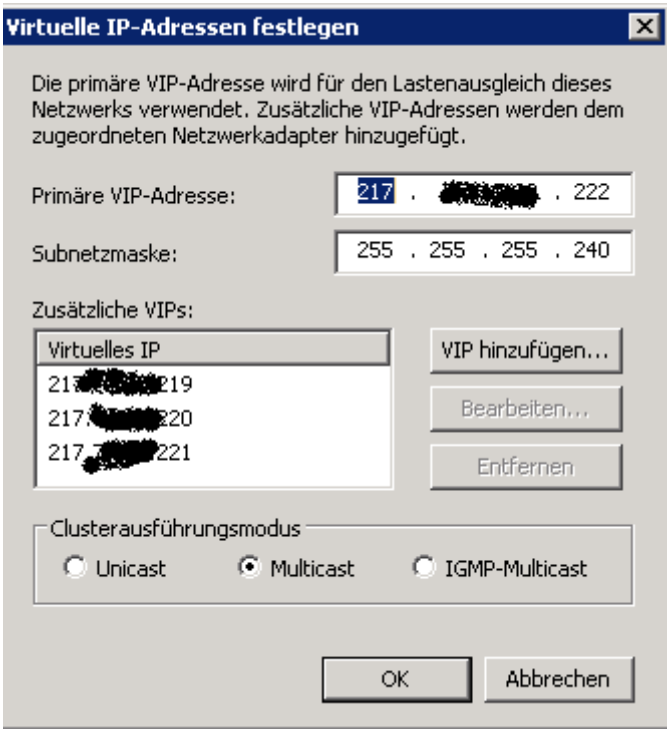
Cache auf dem zweiten Knoten aktivieren



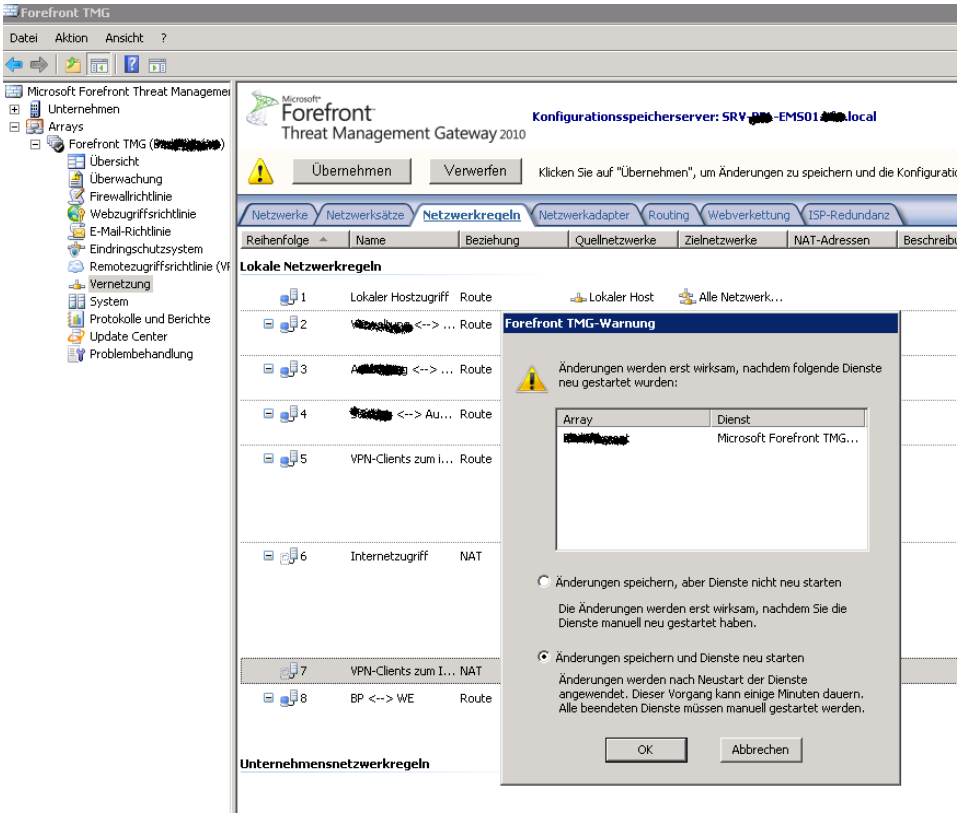
NLB aktivieren



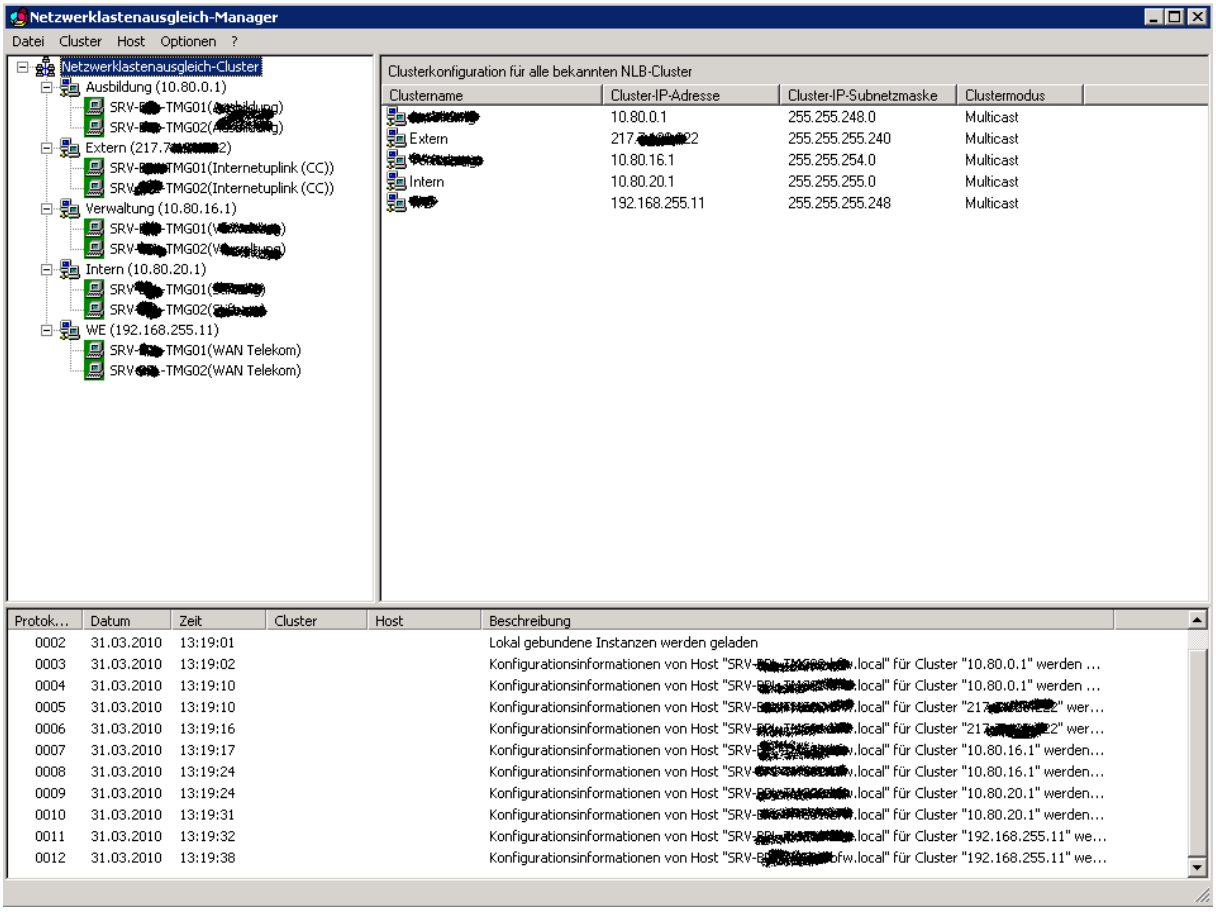
Endlich ☺ - Multicast und Unicast einstellbar ueber GUI. Weiterhin ist die enge Absprache mit den Netzwerkern notwendig, welcher Modus verwendet werden soll!



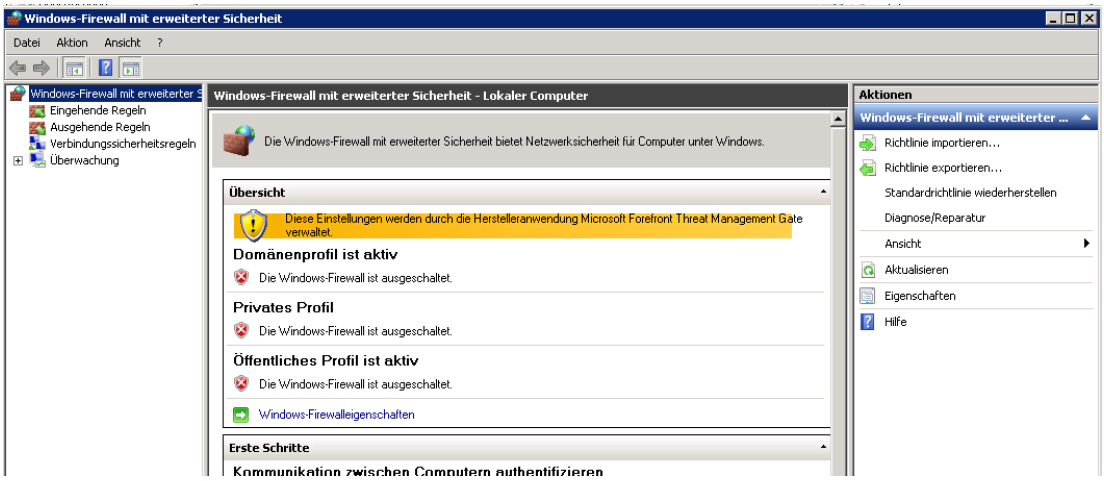
Dienste neu starten, Kaffee trinken oder rauchen und immer beten



NLB Manager Ansicht

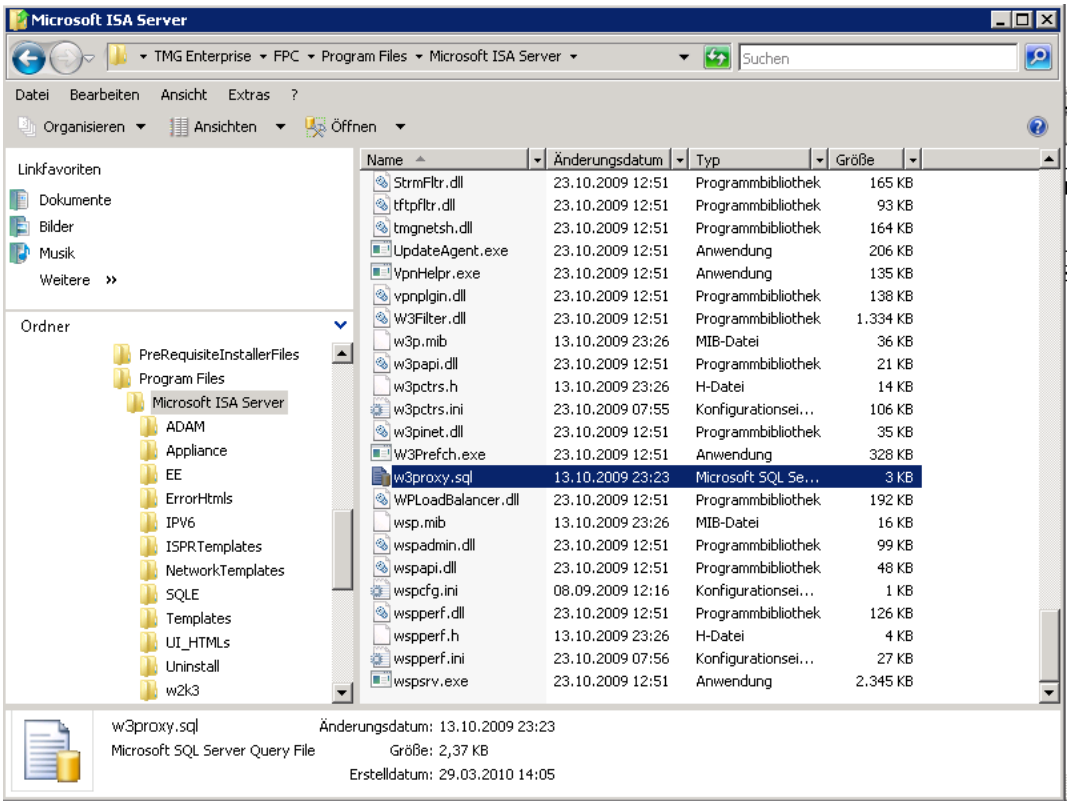


Windows Firewall wird von TMG verwaltet



SQL Server Logging einstellen

Skripte lokalisieren



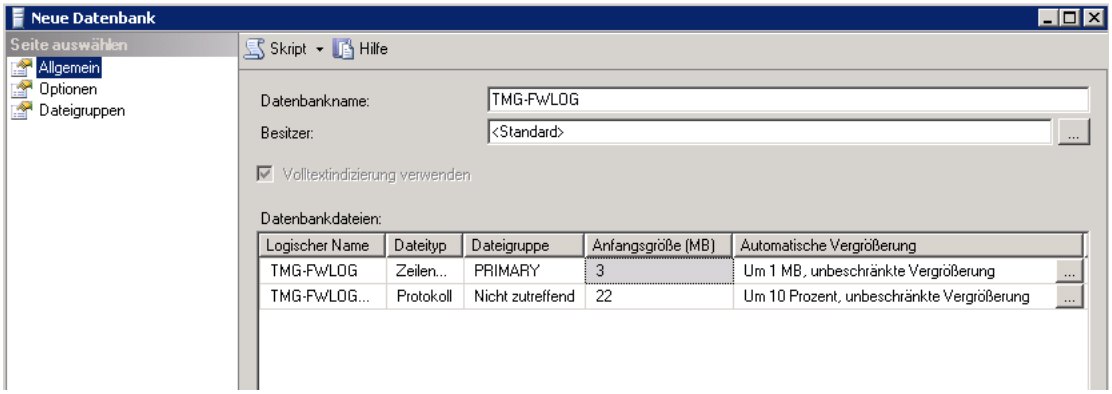
Inhalt

w3proxy.sql - Editor

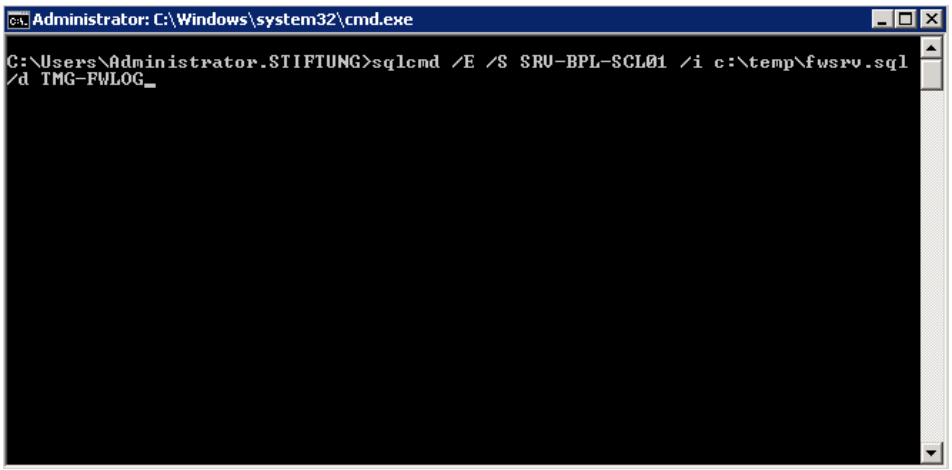
Datei Bearbeiten Format Ansicht ?

```
IF NOT EXISTS (SELECT name FROM sysobjects WHERE name = 'sp_batch_insert' AND type = 'P')
    exec sp_executesql N'CREATE PROCEDURE sp_batch_insert @tempTableName nvarchar(100), @tab
                EXECUTE (''INSERT into ['' + @tableName + ''] SELECT * FROM ['' + @tempTable
                EXECUTE (''truncate table ['' + @tempTableName + '']'')'
GO

IF NOT EXISTS (SELECT name FROM sysobjects WHERE name = 'sp_batch_discard' AND type = 'P')
    exec sp_executesql N'CREATE PROCEDURE sp_batch_discard @tempTableName nvarchar(100) AS
                EXECUTE (''truncate table ['' + @tempTableName + '']'')'
GO

CREATE TABLE WebProxyLog (
  [ClientIP] uniqueidentifier,
  [ClientUserName] nvarchar(514),
  [ClientAgent] varchar(128),
  [ClientAuthenticate] smallint,
  [logTime] datetime,
  [service] smallint,
  [servername] nvarchar(32),
  [referredserver] varchar(255),
  [DestHost] varchar(255),
  [DestHostIP] uniqueidentifier,
  [DestHostPort] int,
  [processingtime] int,
  [bytesrecvd] bigint,
  [bytessent] bigint,
  [protocol] varchar(13),
  [transport] varchar(8),
  [operation] varchar(24),
  [uri] varchar(2048),
  [mimetype] varchar(32),
  [objectsource] smallint,
  [resultcode] int,
  [CacheInfo] int,
  [rule] nvarchar(128),
  [FilterInfo] nvarchar(256),
```

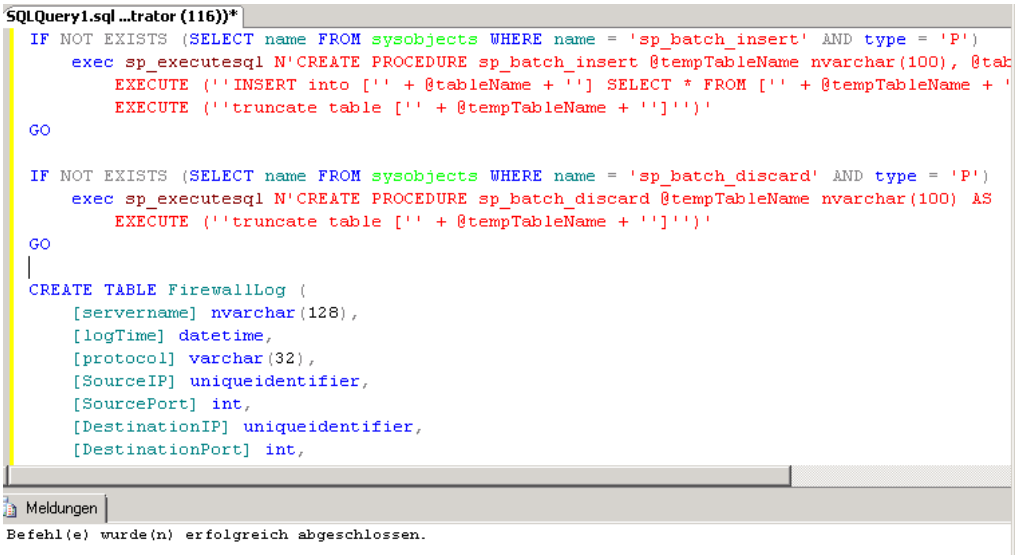
Neue DB fuer Webproxy Log und Firewall Log im Cluster anlegen



Skripte auf dem SQL Cluster ausfuehren



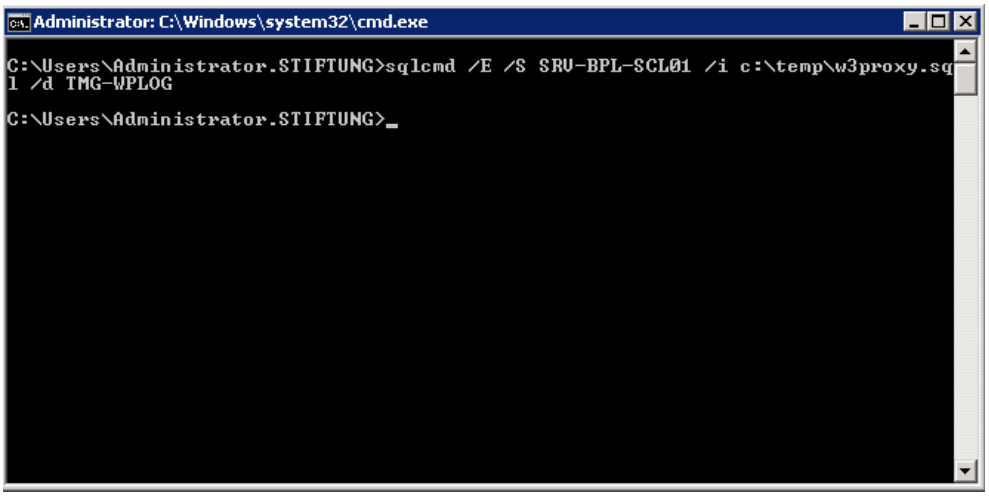
Oder per Management Studio



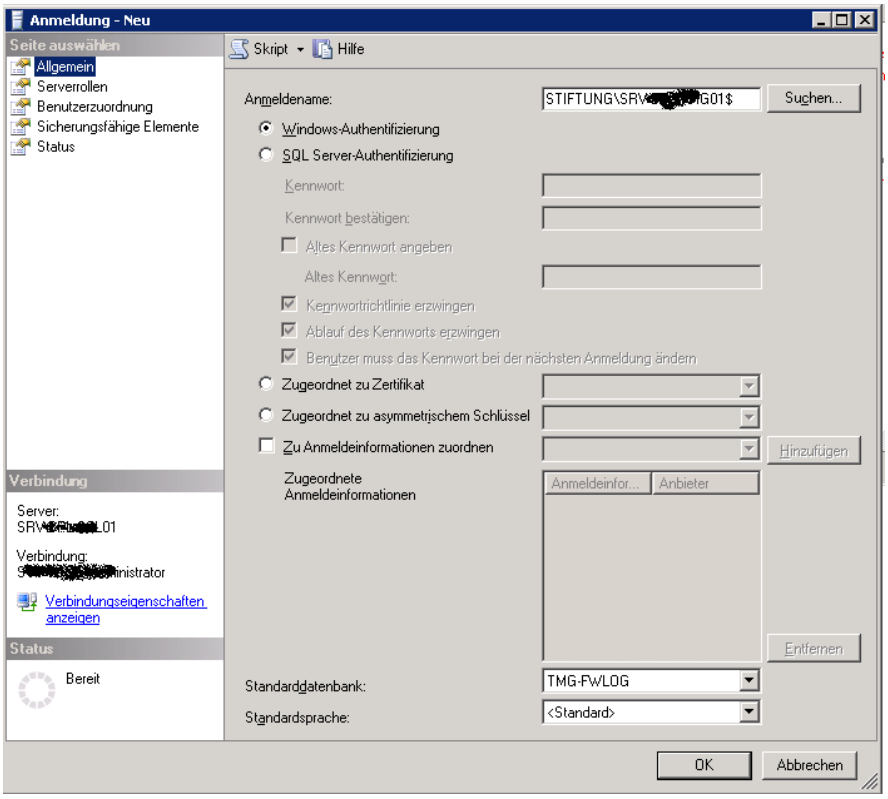
Das gleiche auch nochmal fuer das Webproxy Logging

DB anlegen

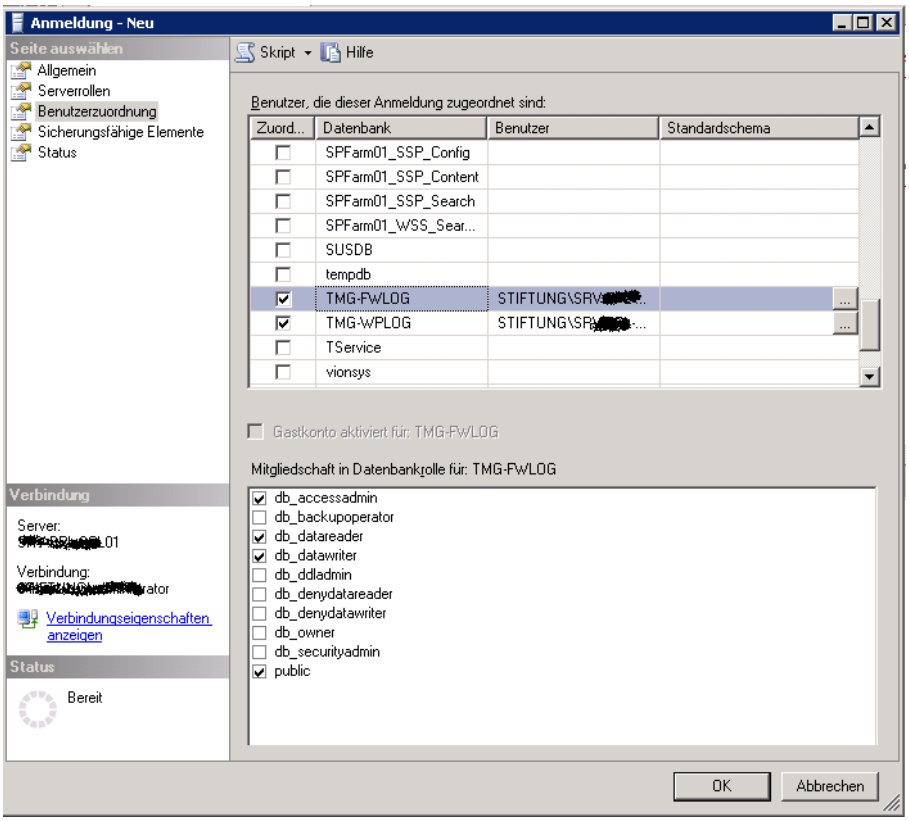
DB mit Tabellen fuellen



Neues SQL Login mit Windows Authentifizierung fuer die TMG Cluster Nodes anlegen

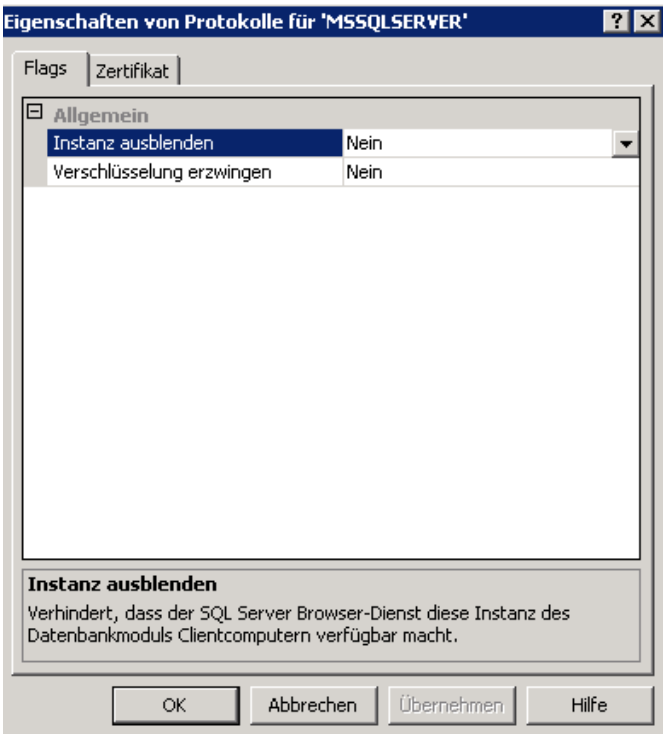


Benoetigte Rechte

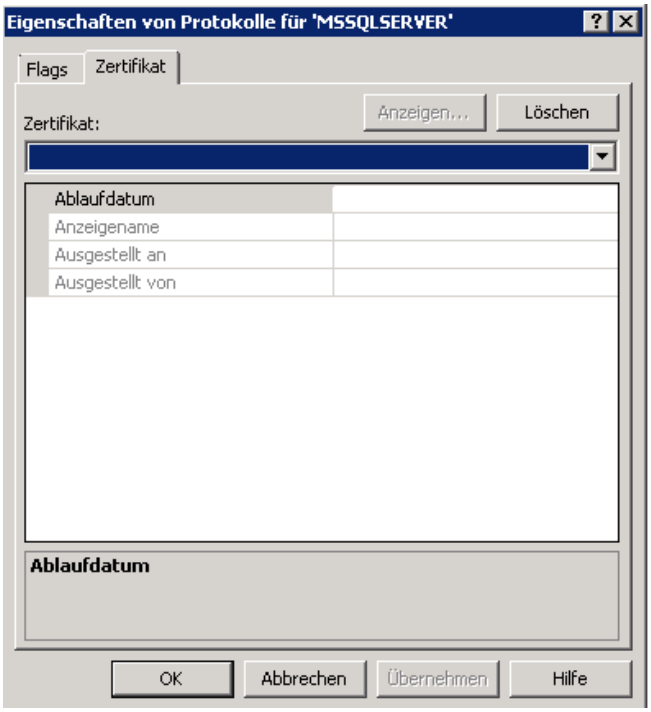


Verschluesselung auf dem SQL Server aktivieren

TMG verwendet standardmaessig eine HTTPS Verschluesselung zum SQL Server. Damit die Verschluesselung funktioniert, benoetigt der SQL Server ein Zertifikat einer RootCA, welcher TMG und SQL vertrauen und die Verschluesselung muss aktiviert werden. Achtung bei Force Encryption, wenn noch andere DB im Cluster liegen (was ja eigentlich der Fall sein sollte ☺.

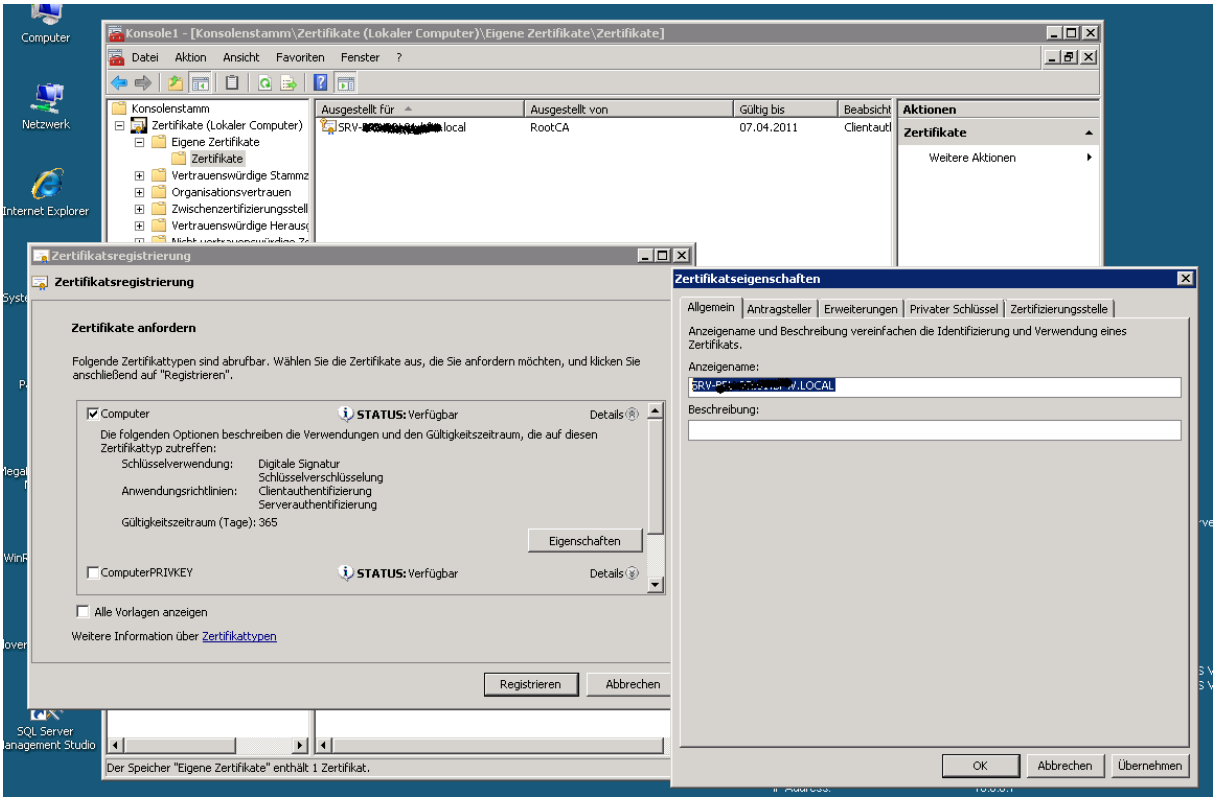


Kein Zertifikat vorhanden

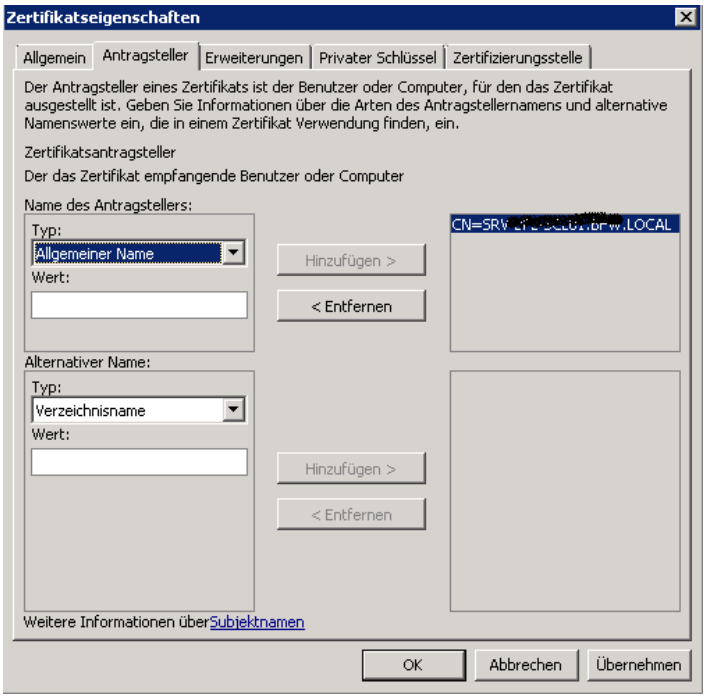


Verschluesselung auf einem Cluster
Wenn Sie die Verschlüsselung für einen Failovercluster verwenden möchten, müssen Sie das Serverzertifikat mit dem vollqualifizierten DNS-Namen der über den Failovercluster verfügenden Instanz auf allen Knoten im Failovercluster installieren. Wenn beispielsweise ein Cluster mit den beiden Knoten **test1.*your company*.com** und **test2.*your company*.com** sowie eine über einen Failovercluster verfügende Instanz von SQL Server mit dem Namen **fcisql** vorliegt, müssen Sie für **fcisql.*your company*.com** ein Zertifikat abrufen und auf beiden Knoten installieren. Anschließend können Sie das Kontrollkästchen **ForceEncryption** im Eigenschaftenfeld **Protokolle für <Server>** der **SQL Server-Netzwerkkonfiguration** aktivieren, um den Failovercluster für die Verschlüsselung zu konfigurieren.

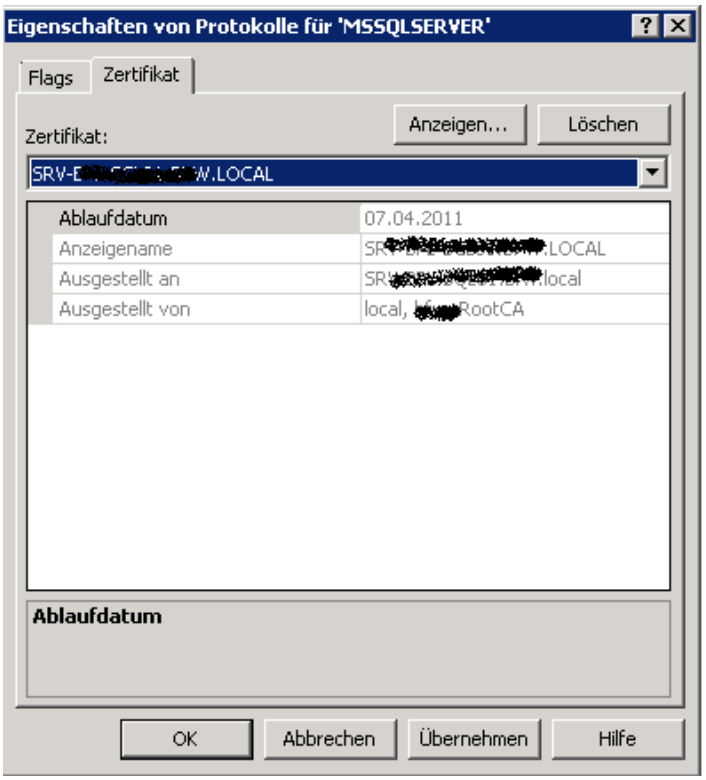
Zertifikat anfordern (lokaler Computer) – auf **ALLEN** SQL Cluster Knoten



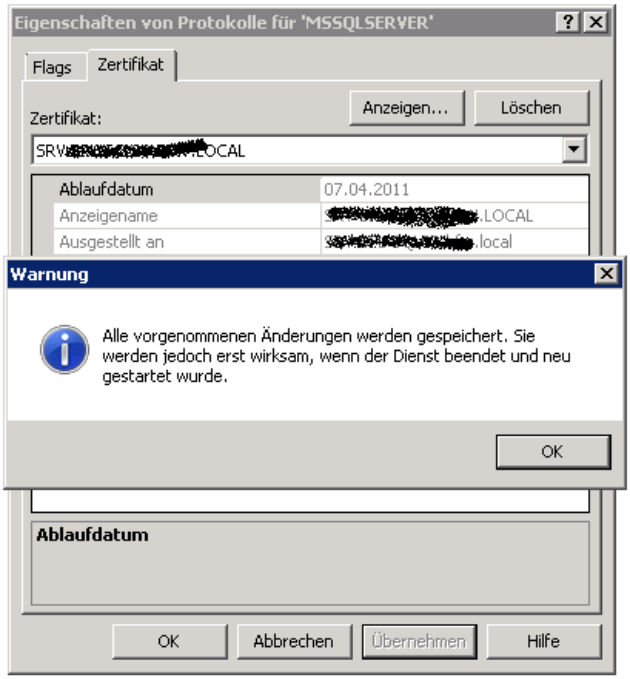
Allgemeinen Namen angeben und ggfs. SAN



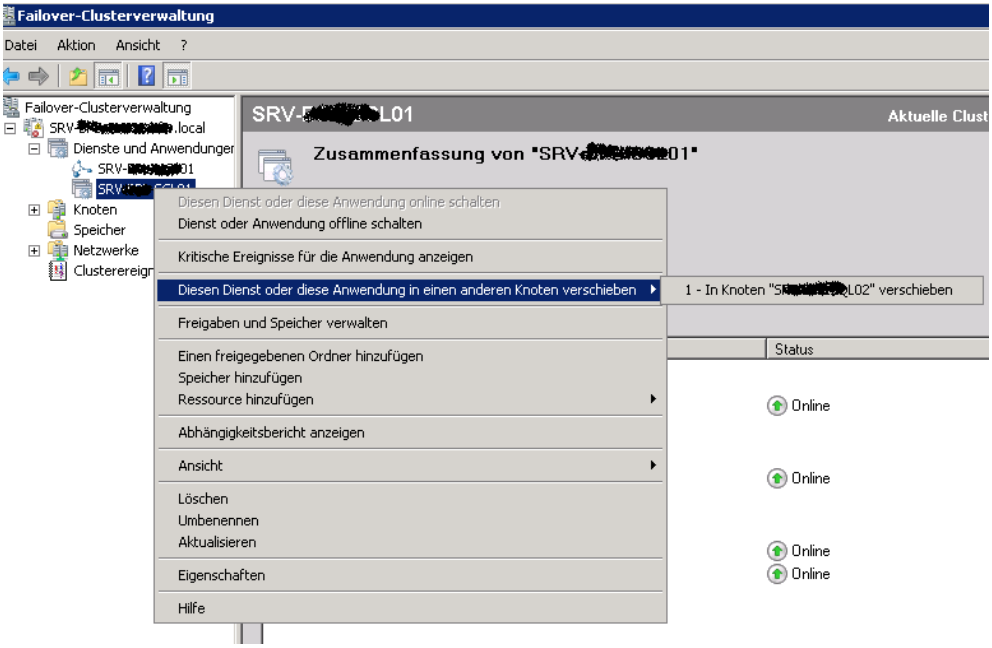
Jetzt kann auch das Zertifikat ausgewaehlt werden



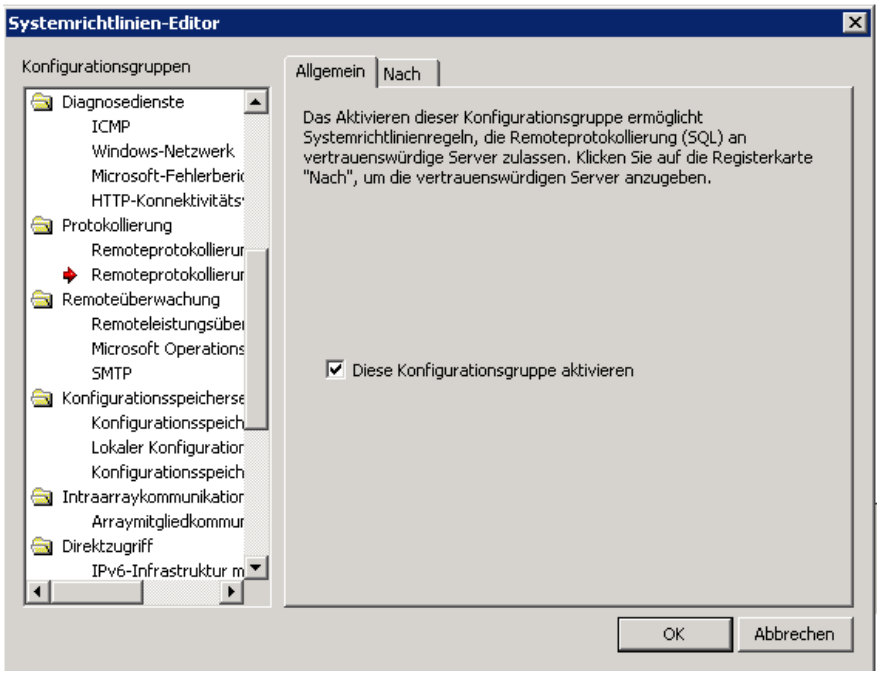
Auch auf dem zweiten SQL Node aktivieren



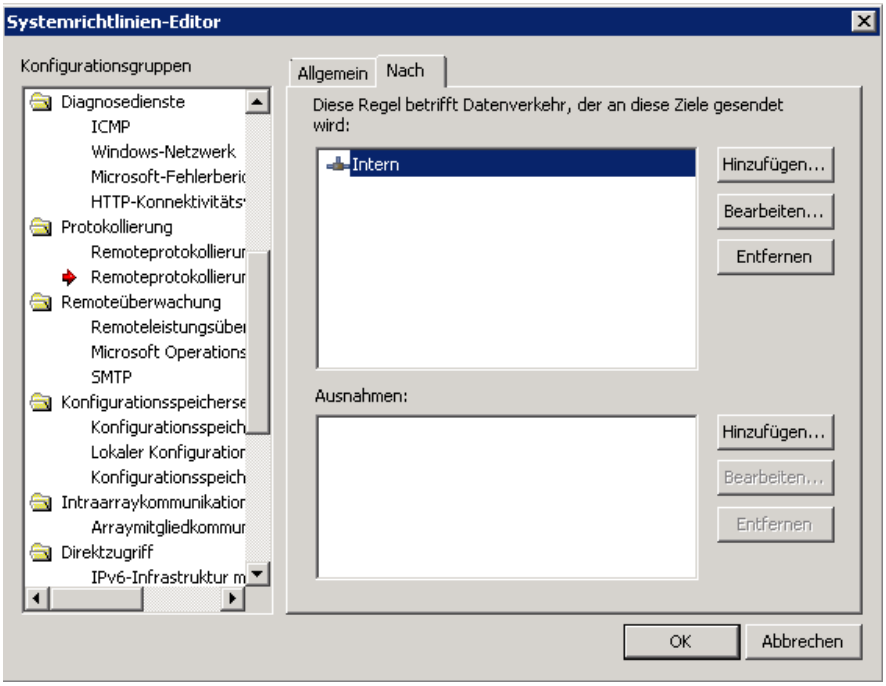
Also einmal einen SQL Cluster Schwenk durchfuehren und die SQL Dienste neu starten



TMG System Policy konfigurieren, das Remote SQL Logging erlaubt ist

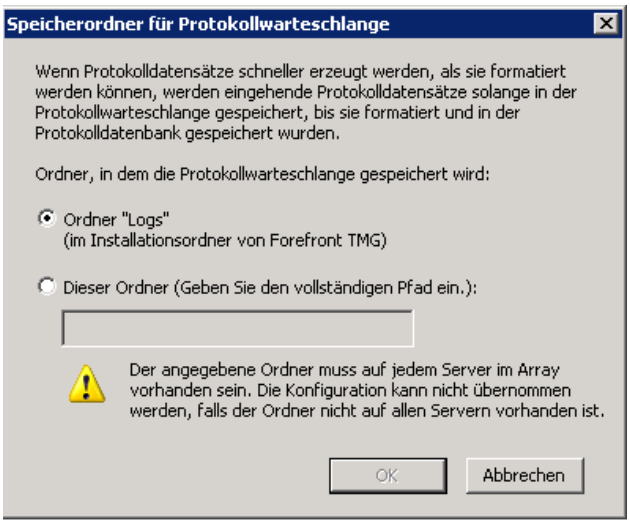


INTERN anpassen auf die SQL Nodes und Cluster Virtual Name / IP



Large Logging Queue (LLQ)

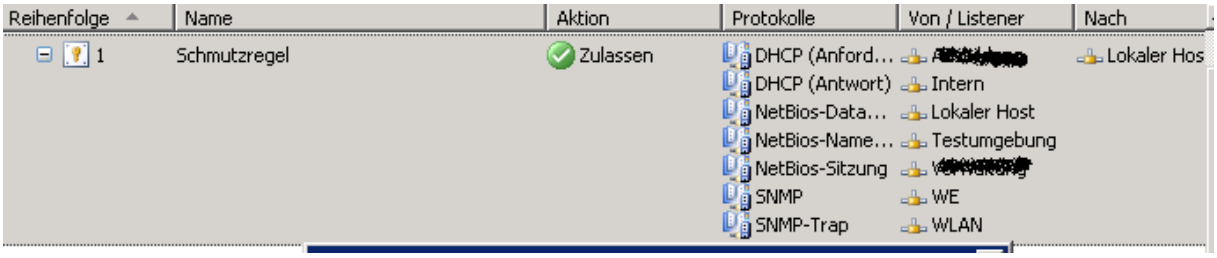
Wenn TMG nicht in den Remote SQL Server loggen kann, werden die Logs lokal zwischengespeichert. Hier sollte fuer ausreichend Plattenplatz auf den TMG Servern gesorgt werden.



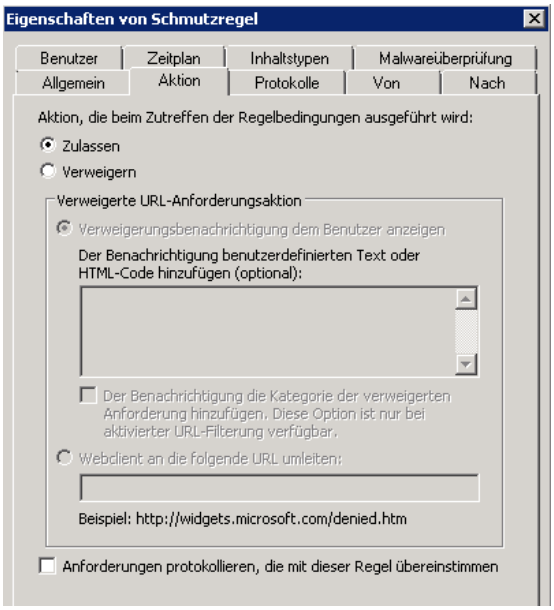
Damit wird verhindert das der TMG in den Firewall Lockdown Modus geht

Weitere Informationen zum TMG Firewall Lockdown Modus
http://www.isaserver.org/tutorials/Explaining-Microsoft-Forefront-TMG-Firewall-Lockdown-Mode.html

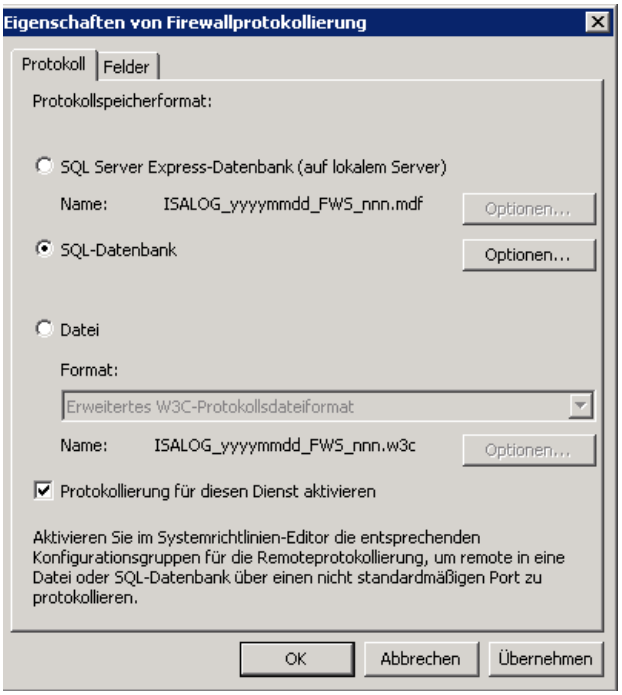
Da TMG sehr viel loggt, kann es Sinn machen, sogenannte Schmutzregeln zu konfigurieren, fuer die nicht notwendiger Traffic (DHCP/NETBIOS etc.) nicht gelogged wird. Damit schont man die Terrabytes auf dem SQL im SAN ☺



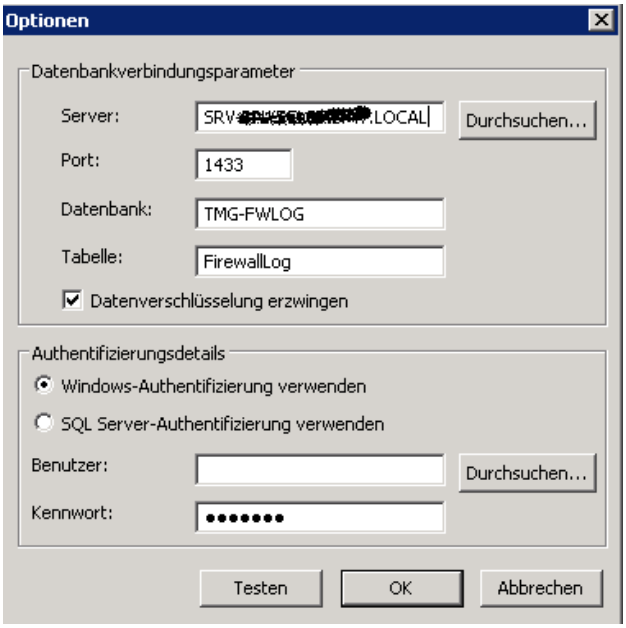
Nicht protokollieren



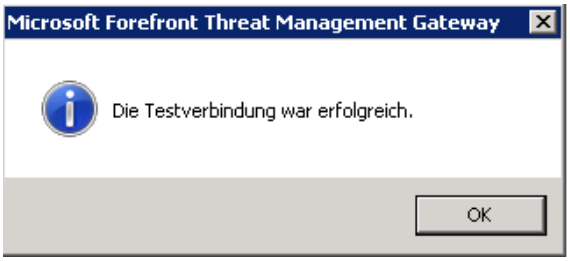
SQL Logging einschalten



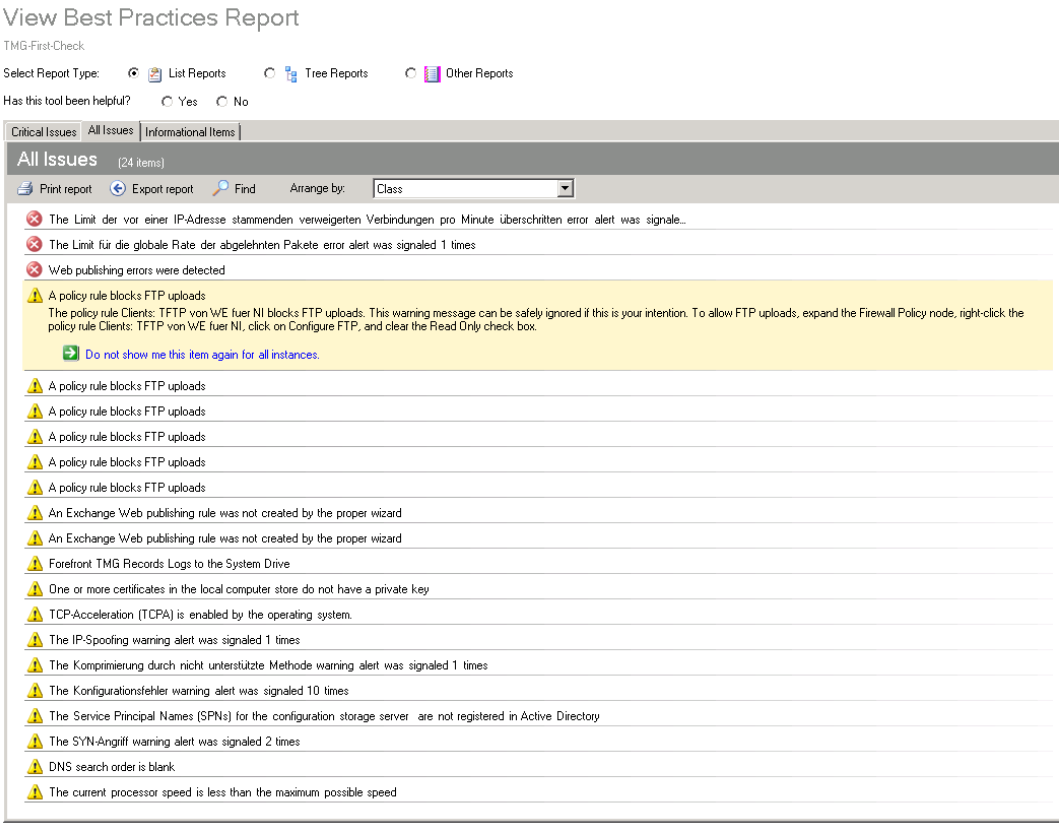
Angabe des virtuellen SQL Server Cluster Objekts



Testen



TMGBPA – es ist alles nicht so schlimm wie es aussieht ☺



Abschlussarbeiten:

- Firewall Policy Regelwerk ueberarbeiten
- Neue TMG Funktionen implementieren
- WPS Lizenz einspielen
- Backup Agents installieren
- Reporting neu einrichten
- SCOM Agent installieren
- Schulung der Administratoren
- Abschlussdokumentation und Abnahme