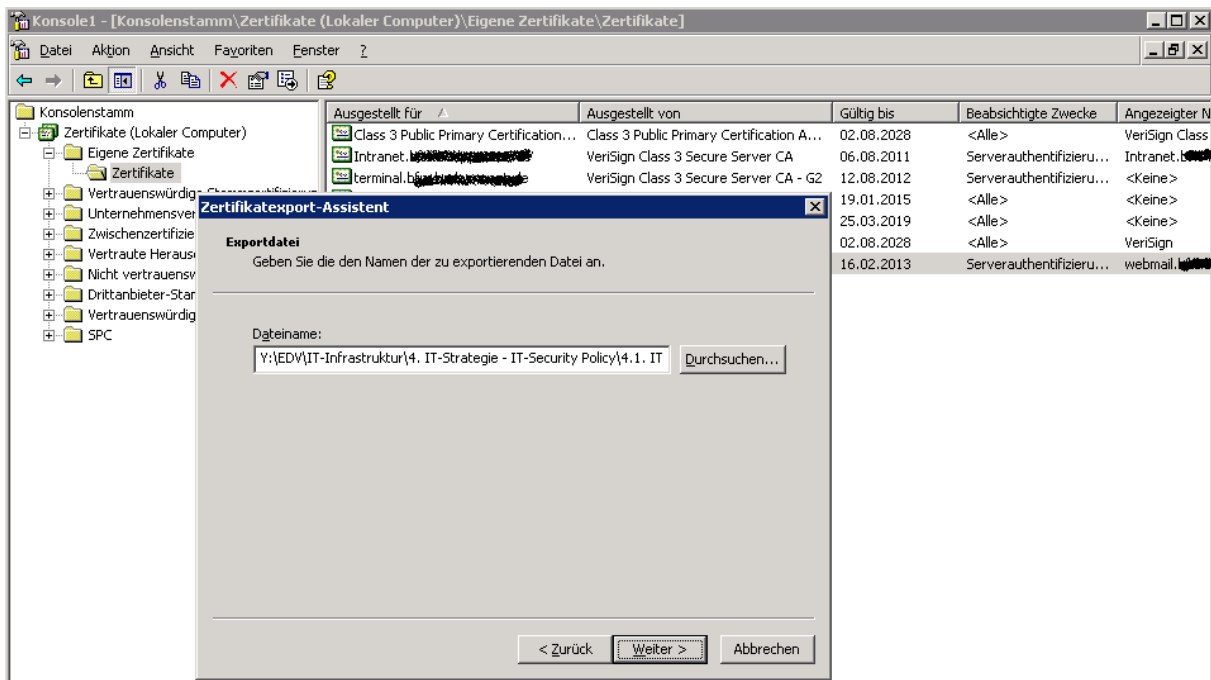


# Forefront TMG EE Migration von ISA Server 2006 EE

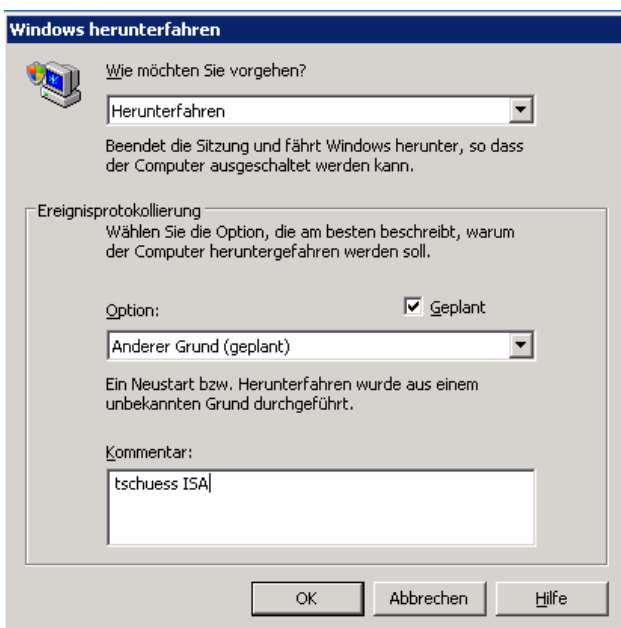
## Erste Schritte

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

## Zertifikate exportieren



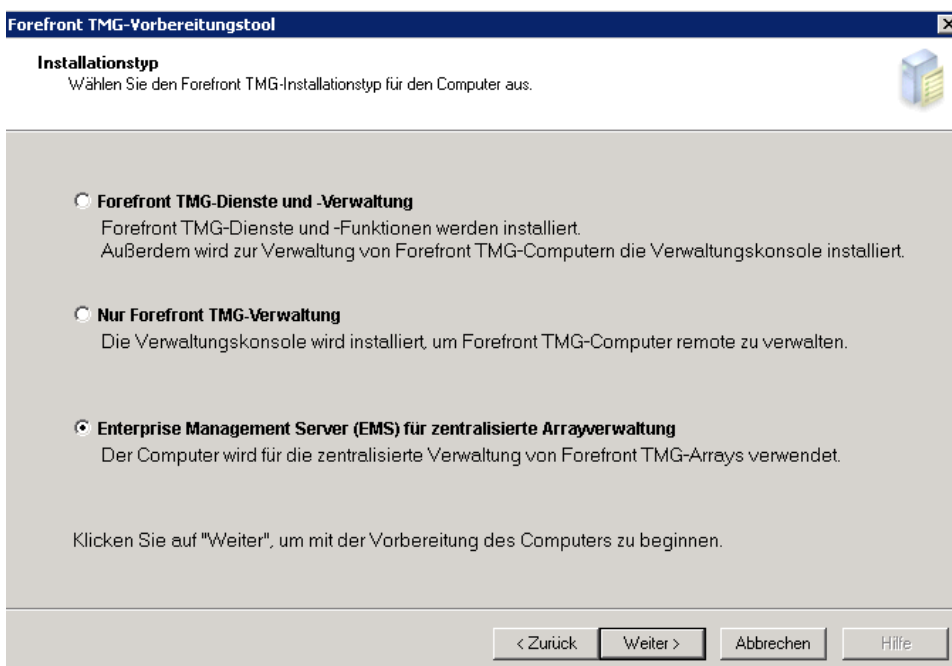
## ISA Server herunterfahren



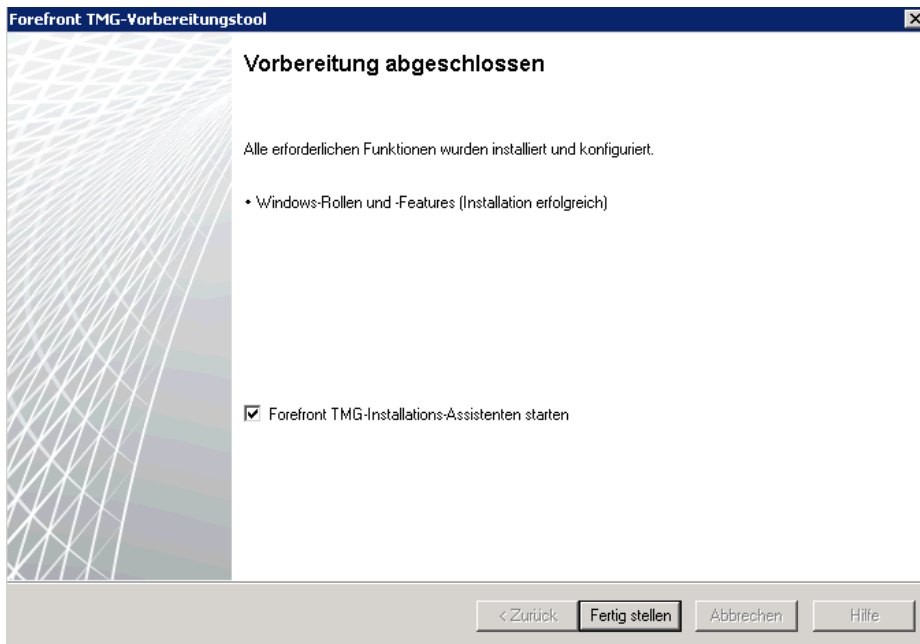
## EMS Installation



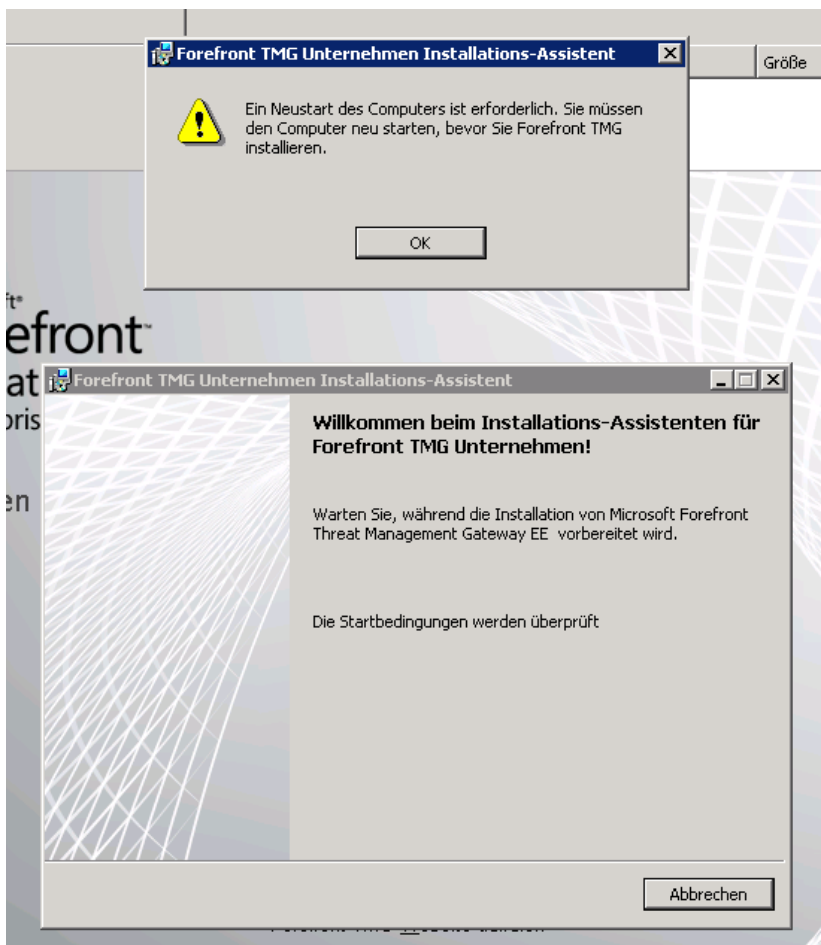
## Vorbereitungstools ausführen



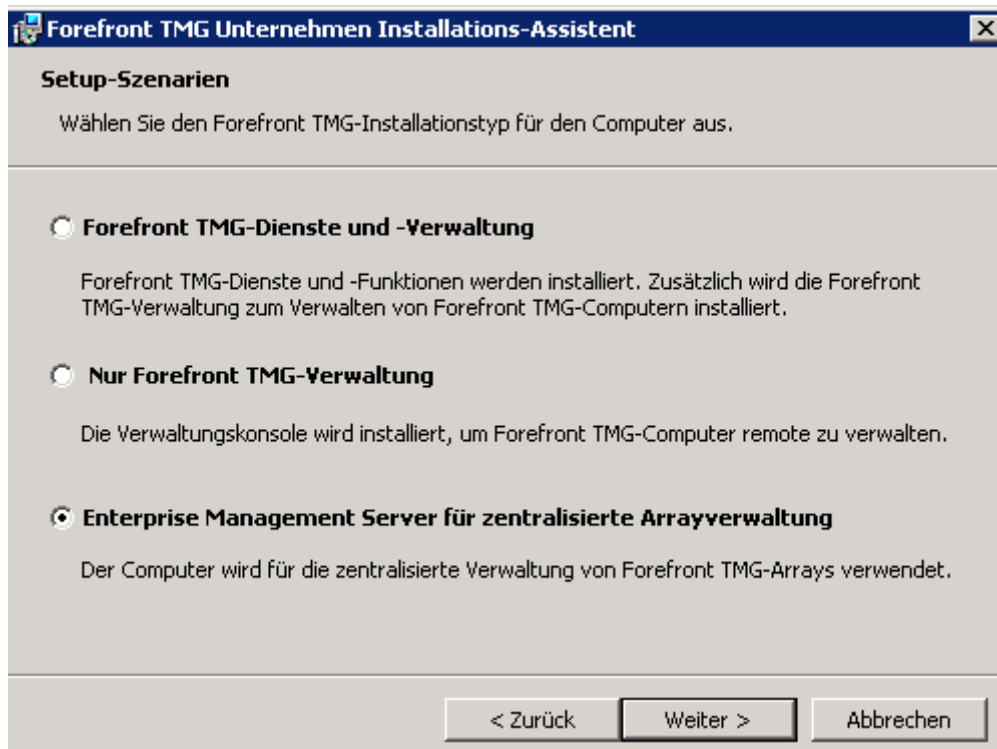
## Installationsassistenten starten



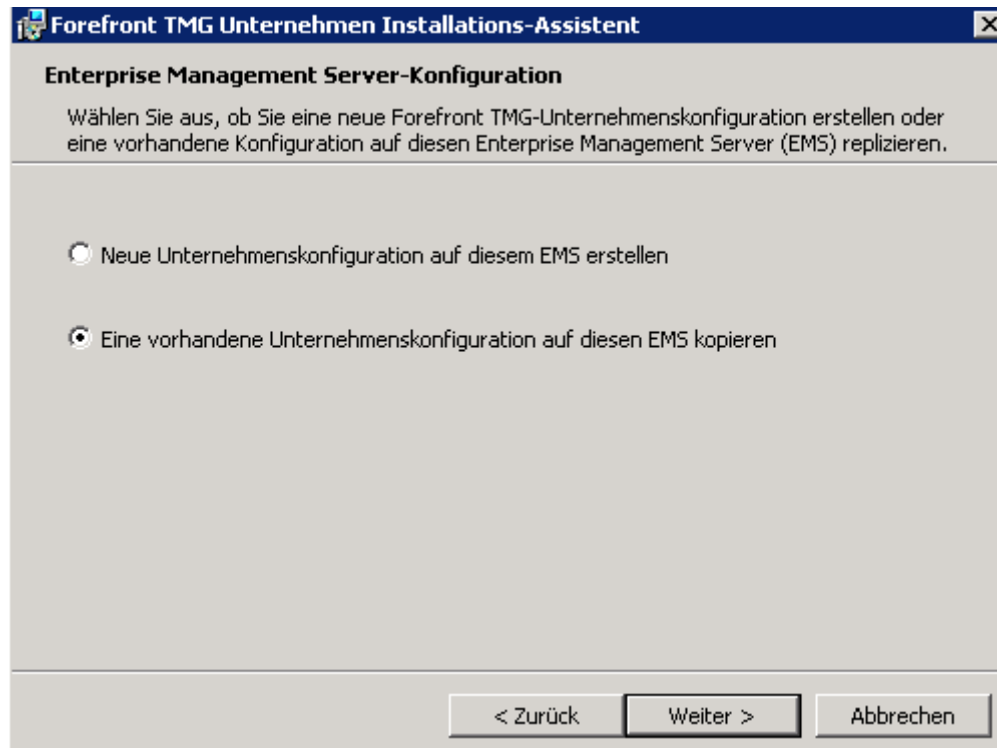
## Neustart erforderlich



## EMS installieren



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



## Konfigurationsspeicherserver replizieren, damit der EMS Zugriff hat

The screenshot shows the Microsoft Internet Security and Acceleration Server 2006 configuration console. A dialog box titled 'Eigenschaften von Konfigurationsspeicherserver replizieren' is open, showing the 'Allgemein' tab. The dialog box contains the following information:

- Name:** Konfigurationsspeicherserver replizieren
- In diesem Computersatz enthaltene Computer, Adressbereiche und Subnetze:**

Name	IP-Adressen
srv-...	192.168.1.0/24
srv-...	192.168.2.0/24
srv-...	192.168.3.0/24
SRV-EM501	192.168.4.0/24
- Beschreibung (optional):** Alle Konfigurationsspeicherserver, die mit dem lokalen Konfigurationsspeicherserver repliziert werden.
- Bereich:** Unternehmen

The dialog box also has buttons for 'Hinzufügen...', 'Bearbeiten...', and 'Löschen'. At the bottom, there are 'OK', 'Abbrechen', and 'Übernehmen' buttons.

## Angabe des CSS

The screenshot shows a dialog box titled 'Mehrere Namen gefunden'. The text inside the dialog box reads: 'Mehrere Objekte stimmen mit dem Namen "srv-..." überein. Wählen Sie mindestens ein Objekt aus der Liste aus., oder geben Sie den Namen erneut ein.'

Below the text, there is a section titled 'Übereinstimmende Namen:' followed by a table:

Name (RDN)	Beschreibung	Ordner
SRV-...	ISA-Server 01	...
SRV-...	ISA-Server 02	...

At the bottom of the dialog box, there are 'OK' and 'Abbrechen' buttons.

## Suchen des Konfigurationsspeicherservers

**Forefront TMG Unternehmen Installations-Assistent**

**Konfigurationsspeicherserver suchen**

Legen Sie den Konfigurationsspeicherserver für die Replikation und die Anmeldeinformationen für die Verbindung mit dem Server fest.

Konfigurationsspeicherserver (vollständigen Domännennamen eingeben):

srv-1234567890.local

Anmeldeinformationen für Verbindung

Über die Anmeldeinformationen des angemeldeten Benutzers verbinden

Über dieses Konto verbinden:

Benutzername:

Kennwort:


< Zurück Weiter > Abbrechen

## ACHTUNG:

**Forefront TMG Unternehmen Installations-Assistent**

**Konfigurationsreplikation - Warnung**

Der für die Replikation ausgewählte Konfigurationsspeicherserver gehört zu einem ISA Server 2006-Unternehmen.

 Wenn die Konfiguration, die für die Installation des Konfigurationsspeicherservers verwendet wird, aus einer früheren Version des Produkts repliziert wird, wird das Produkt im gemischten Unternehmensmodus ausgeführt.

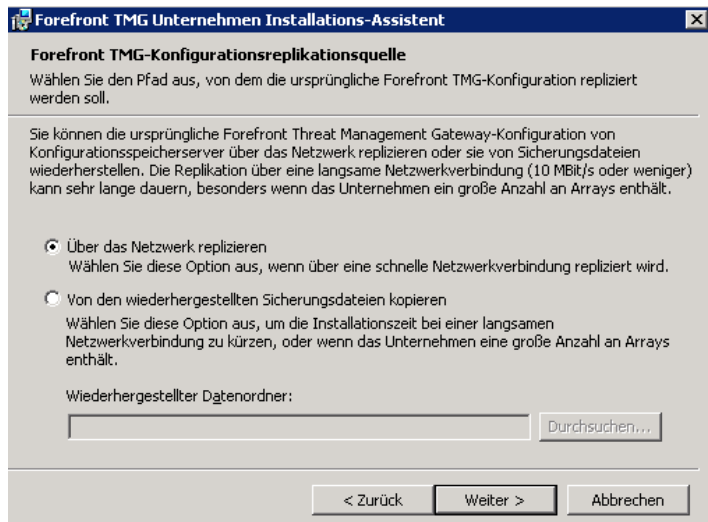
Im gemischten Unternehmensmodus ist die Verwaltung auf Unternehmensebene auf ISA Server 2006-Funktionen beschränkt. Darüber hinaus sind Objekte auf Unternehmensebene schreibgeschützt, wenn das Unternehmen von der ISA Server 2006-Verwaltungskonsolle aus verwaltet wird.

Sie sollten sich im Produktbereitstellungshandbuch eingehend über den gemischten Unternehmensmodus informieren, bevor Sie den Vorgang fortsetzen.

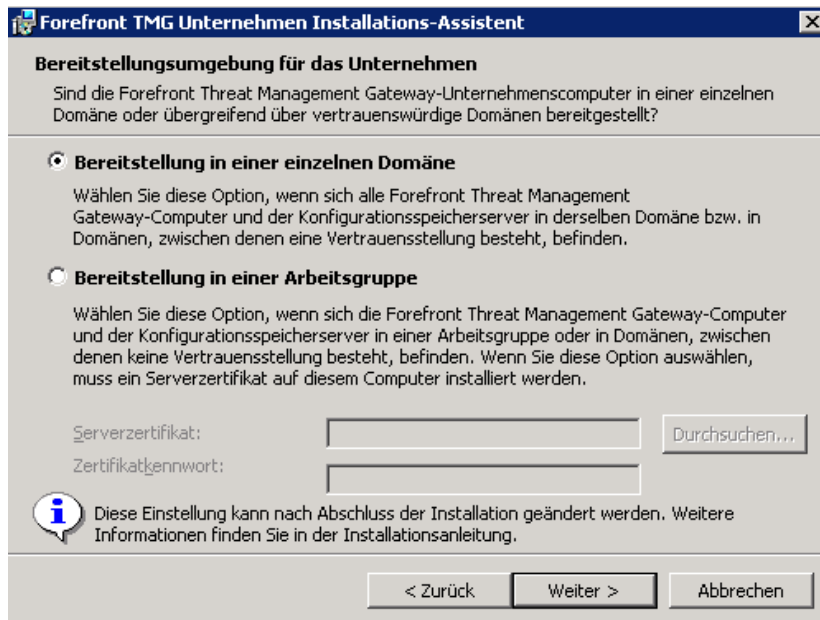
Klicken Sie auf "Zurück", um einen anderen Konfigurationsspeicherserver auszuwählen. Klicken Sie auf "Weiter", um den ausgewählten ISA Server 2006-Konfigurationsspeicherserver zu verwenden.

< Zurück Weiter > Abbrechen

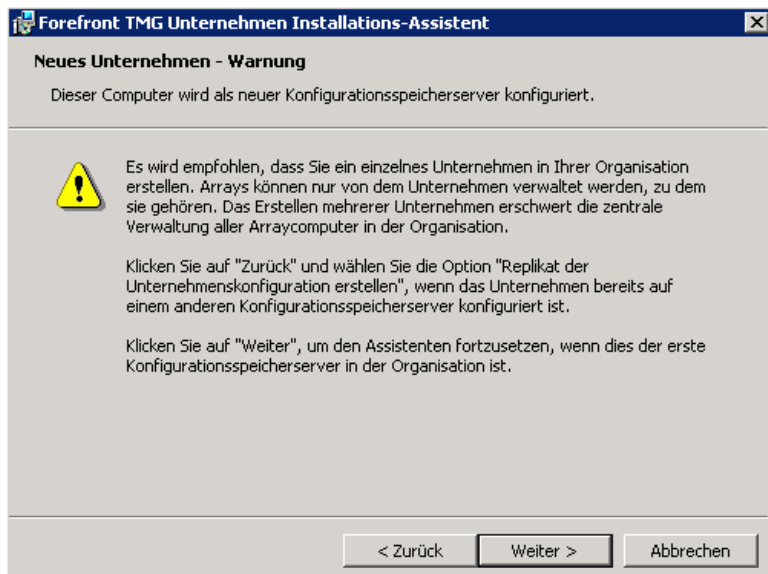
## Ueber das Netzwerk replizieren



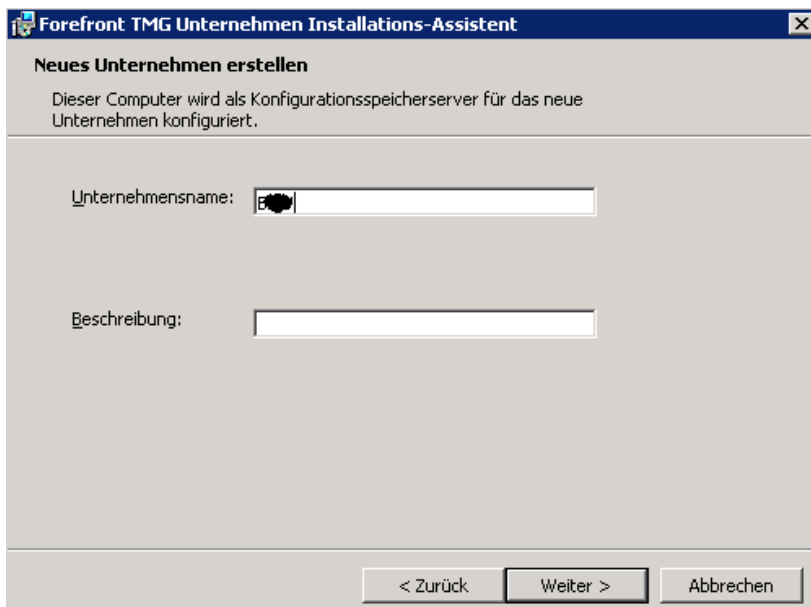
## Bereitstellung in einer einzelnen Domaene



Hinweis, dass keine multiplen Forefront TMG Unternehmen erstellt werden sollten

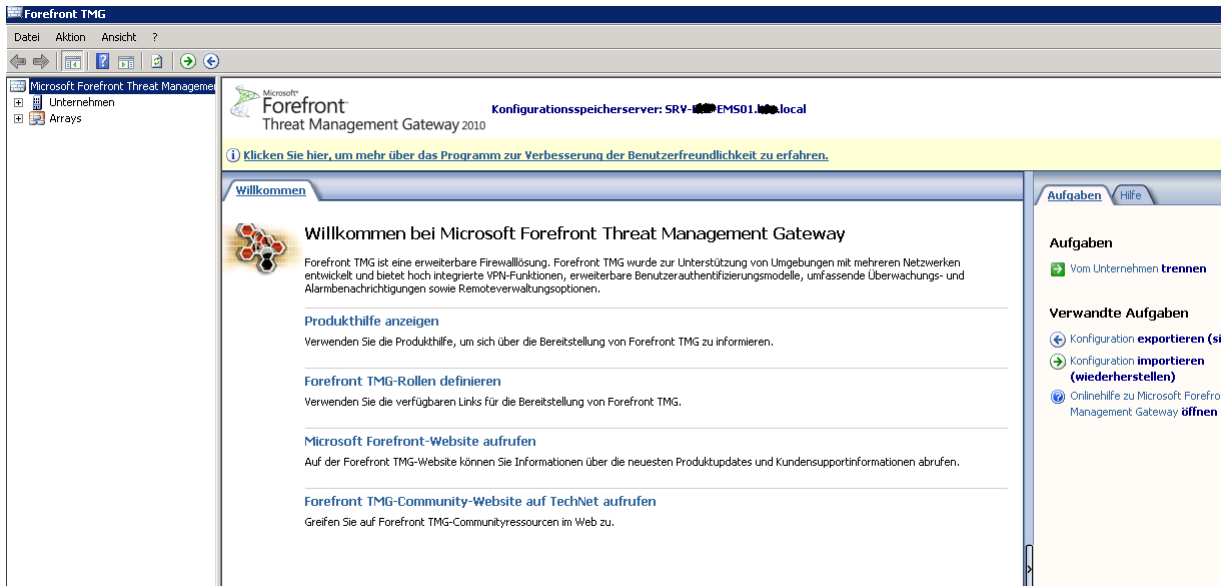


## TMG Enterprise neu erstellen

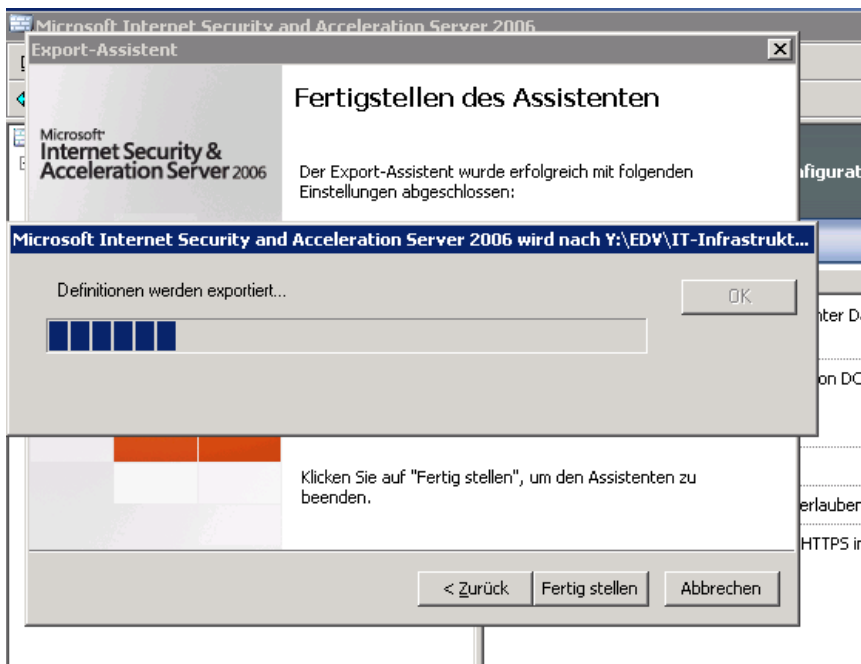


Danach kann die TMG-Verwaltungskonsole gestartet werden

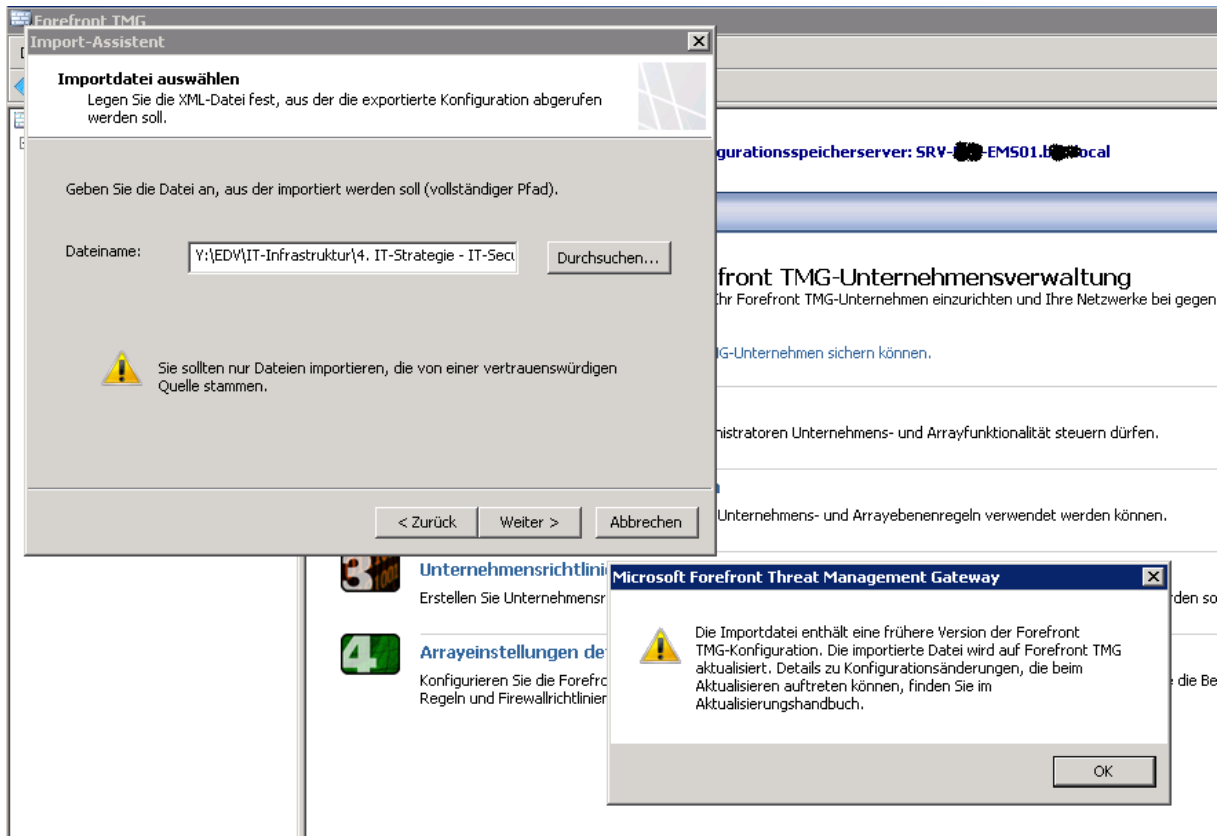




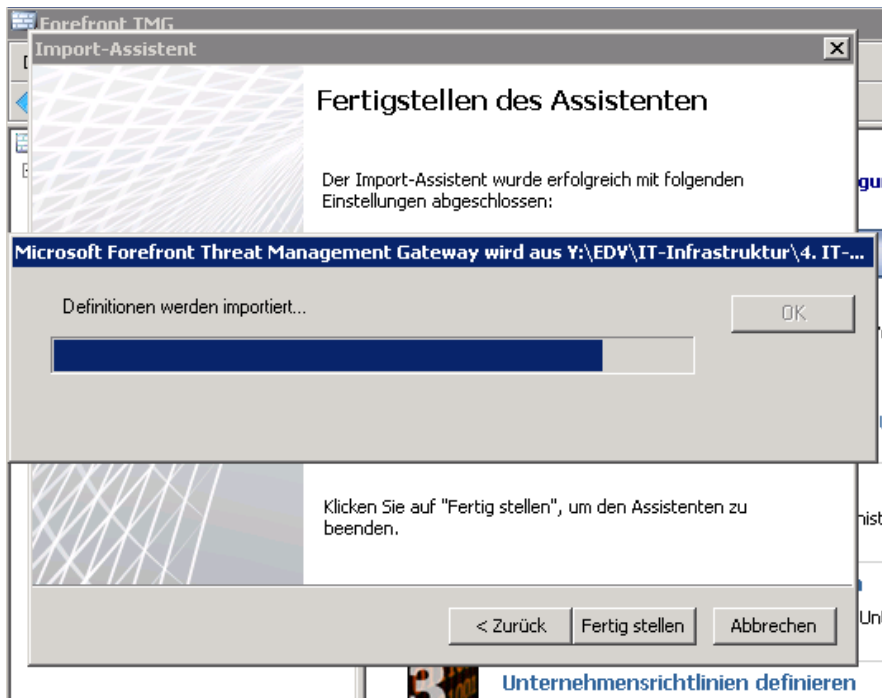
## Export der ISA Server 2006 Konfiguration



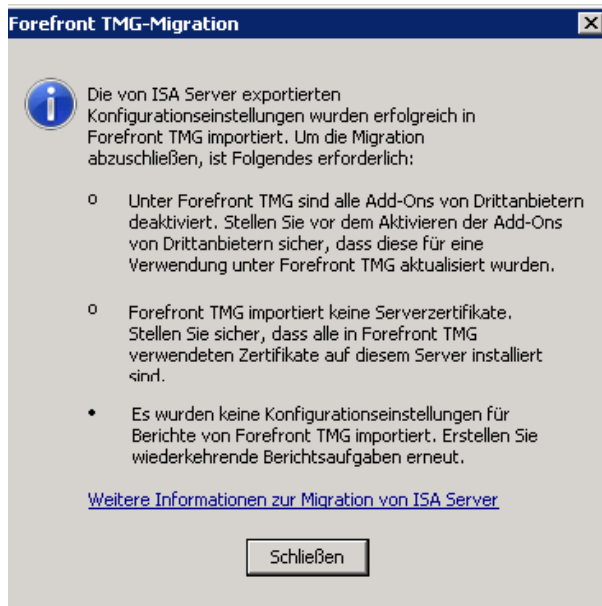
## Import der ISA Konfiguration in den EMS



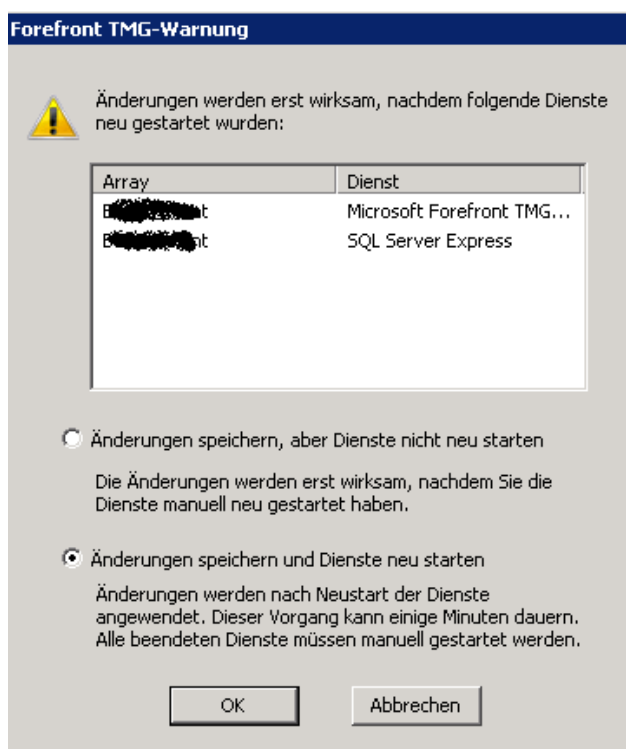
Konfig wird importiert



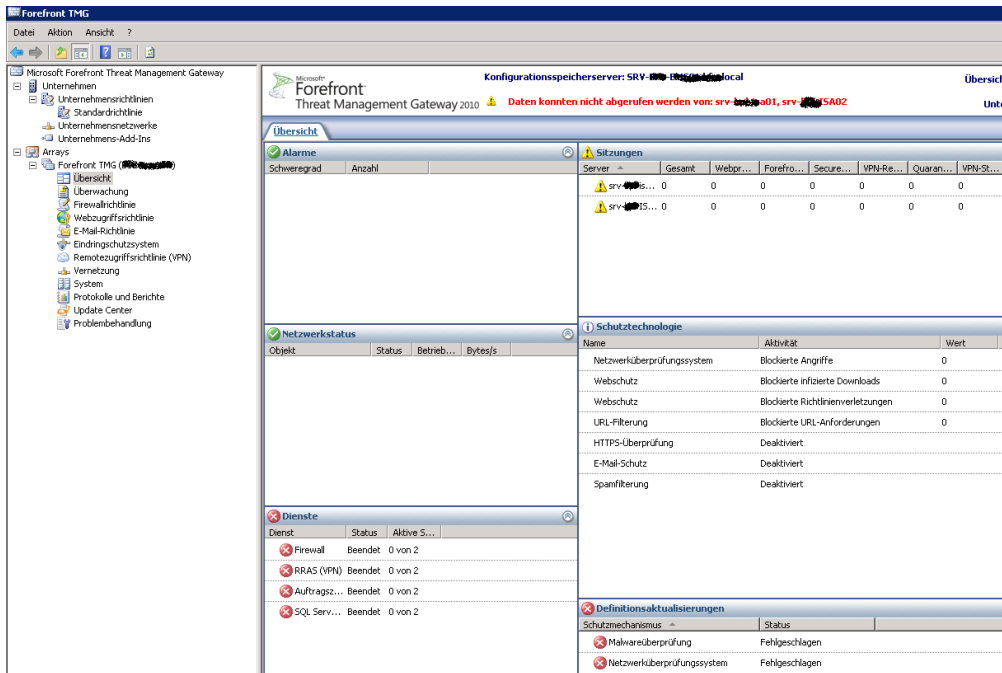
Etwas Nacharbeit ist erforderlich



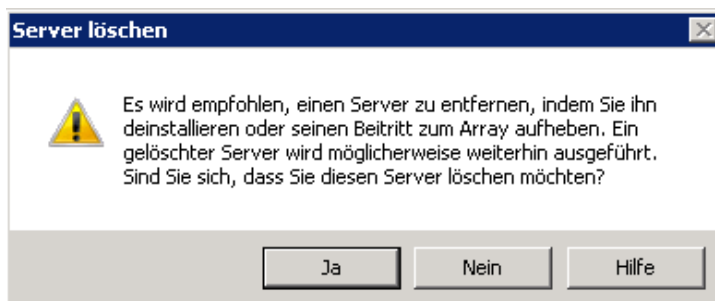
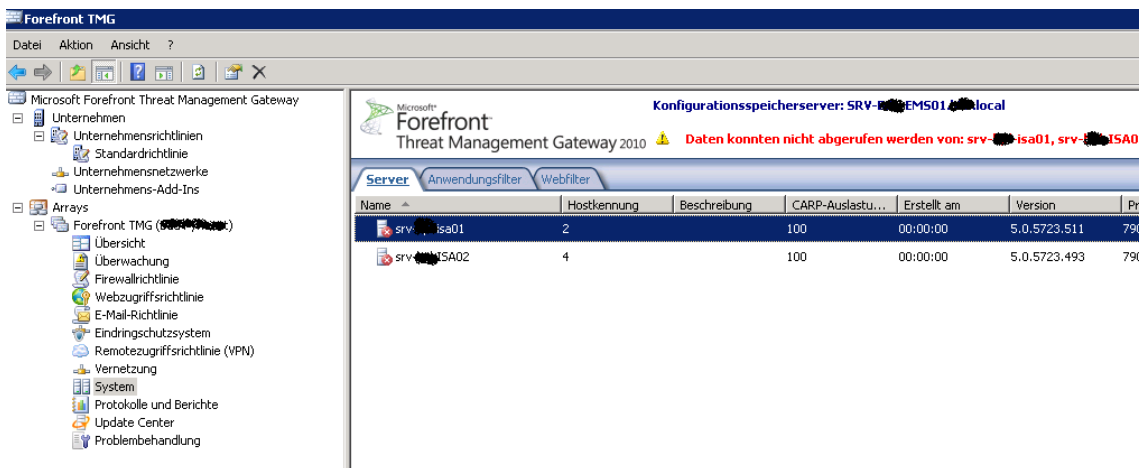
## Konfigurationsänderungen übernehmen und Dienste neu starten



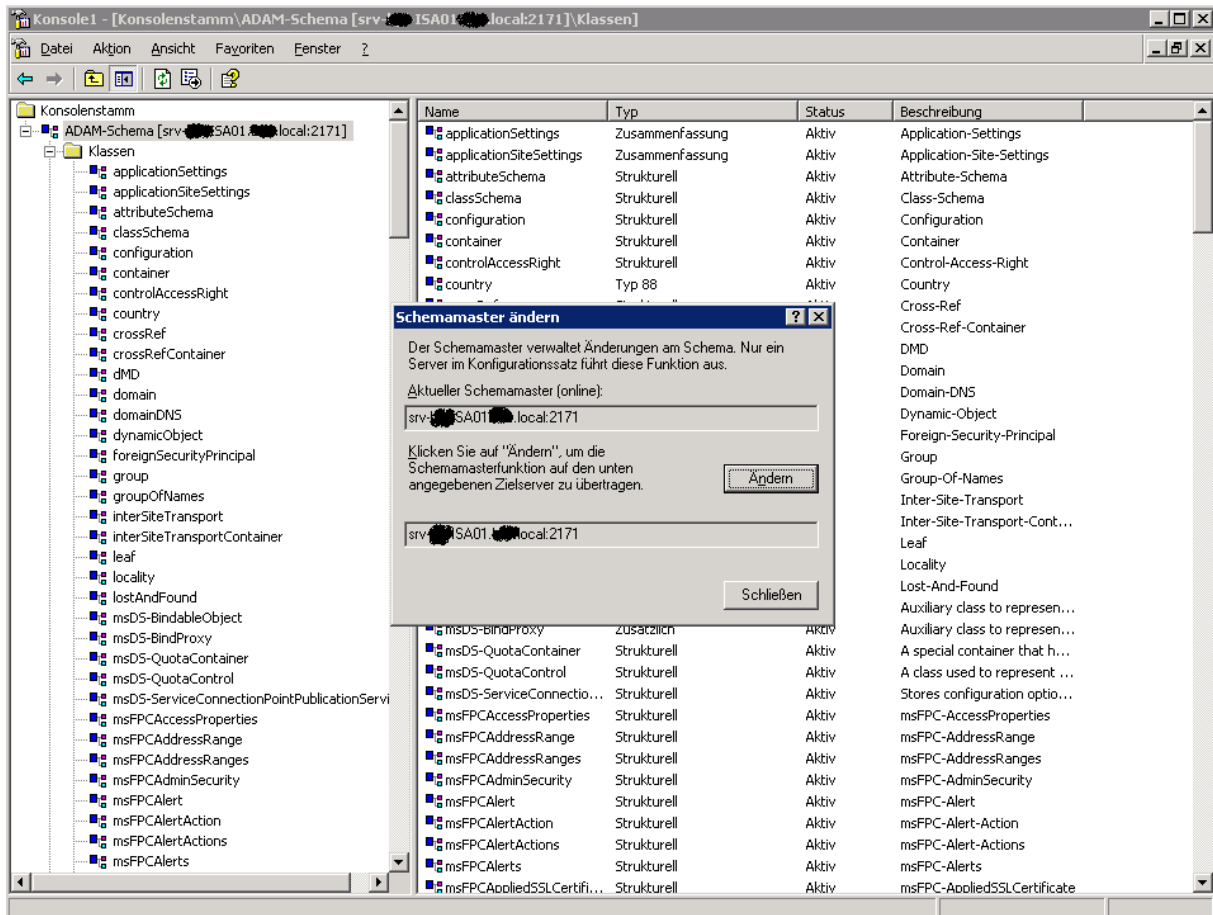
OK, die Server gibt es ja so nicht mehr im Array



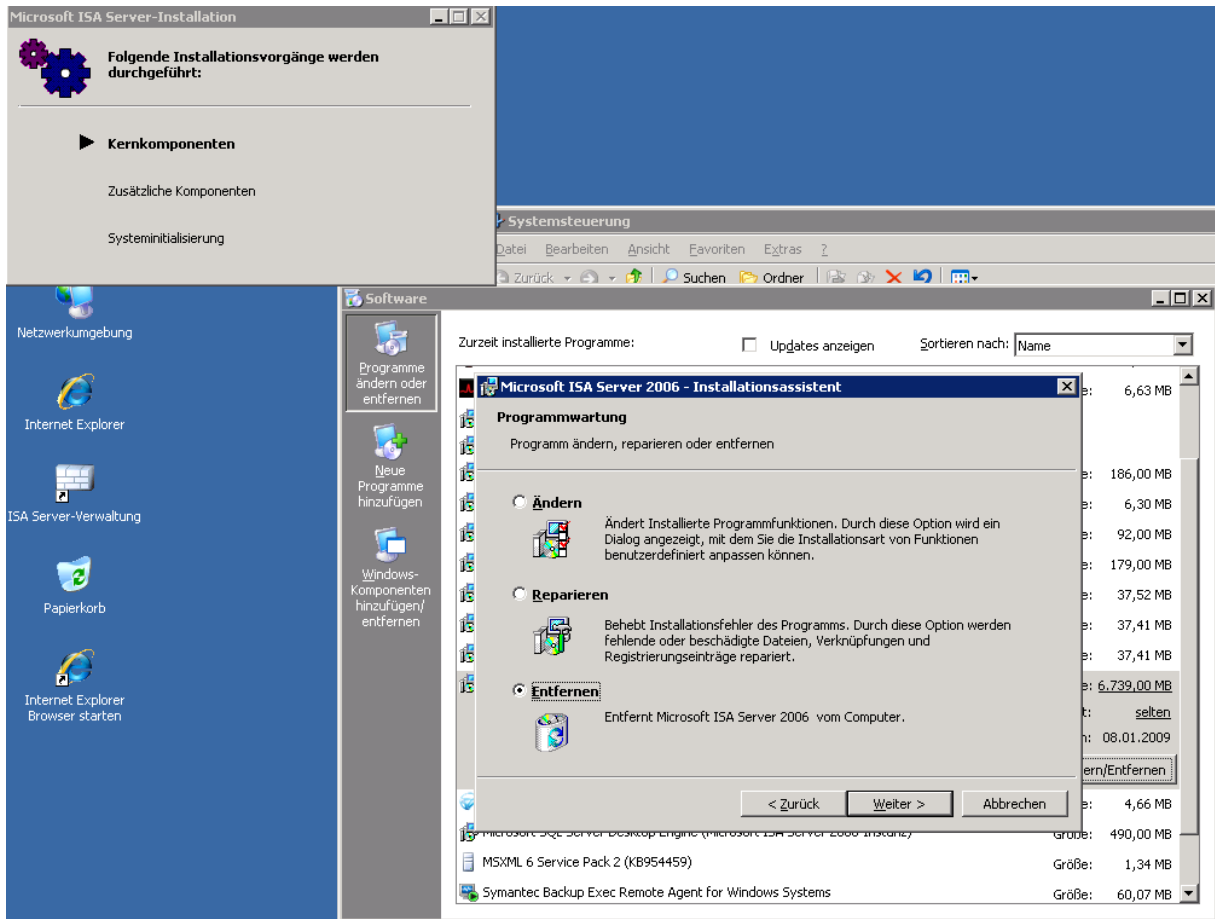
Server löschen, da diese neu installiert werden und auch neue Namen erhalten



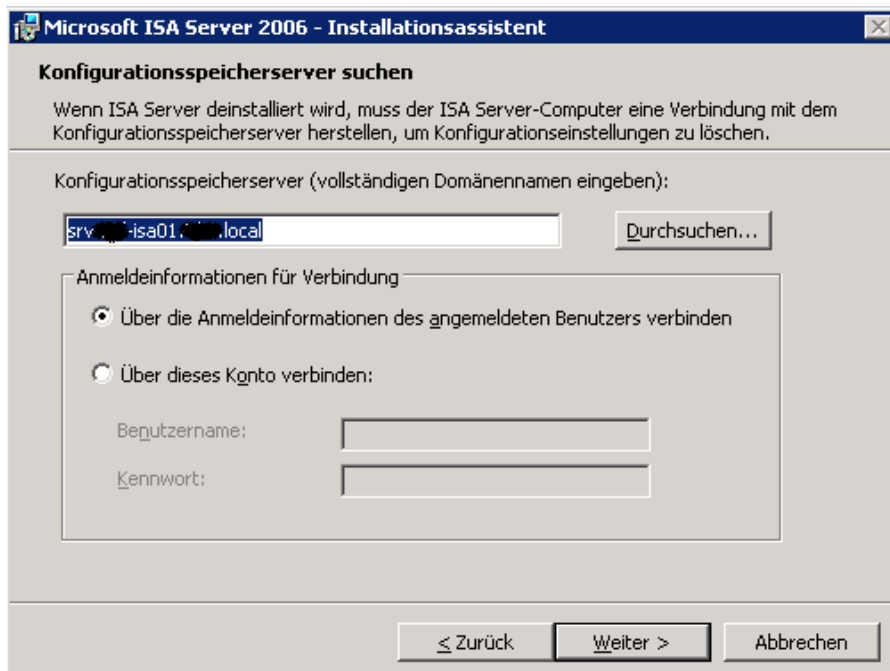
ISA Schema Master auf den Server ändern, welcher als letztes deinstalliert wird



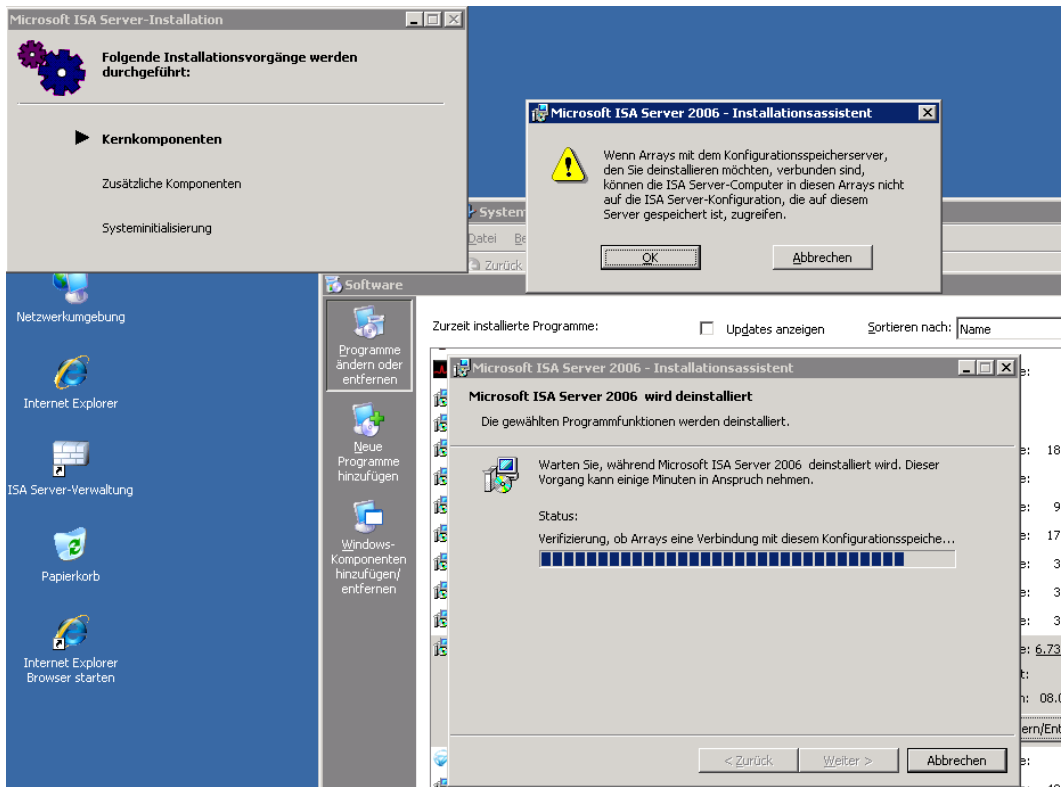
Ersten ISA Server aus dem Array deinstallieren



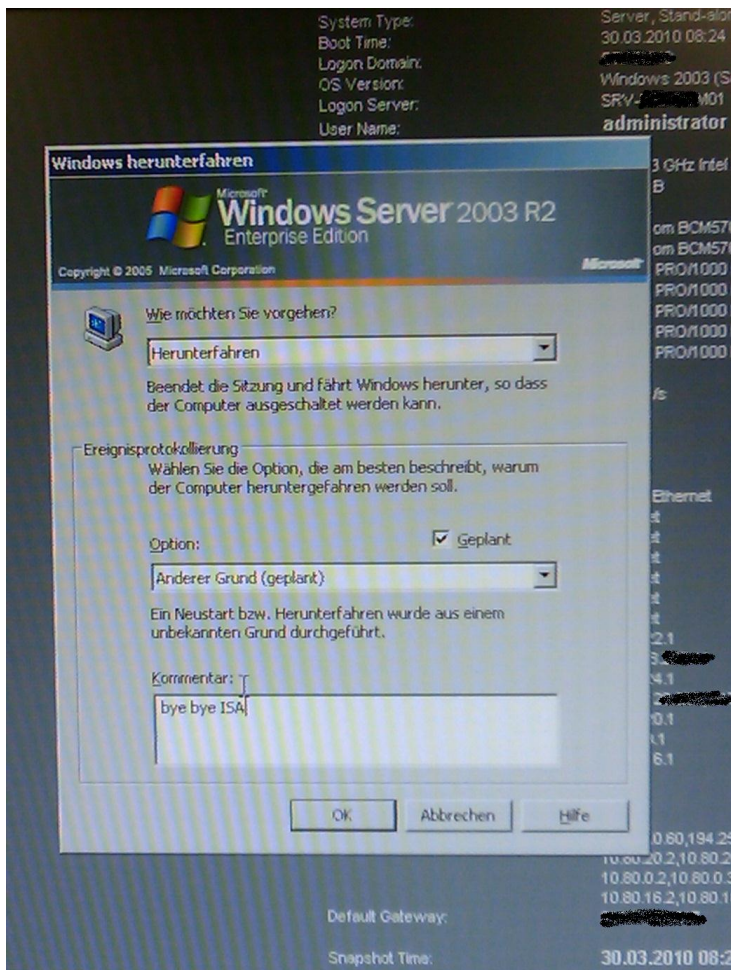
Verbindung mit CSS aufnehmen



Ja, alles weg

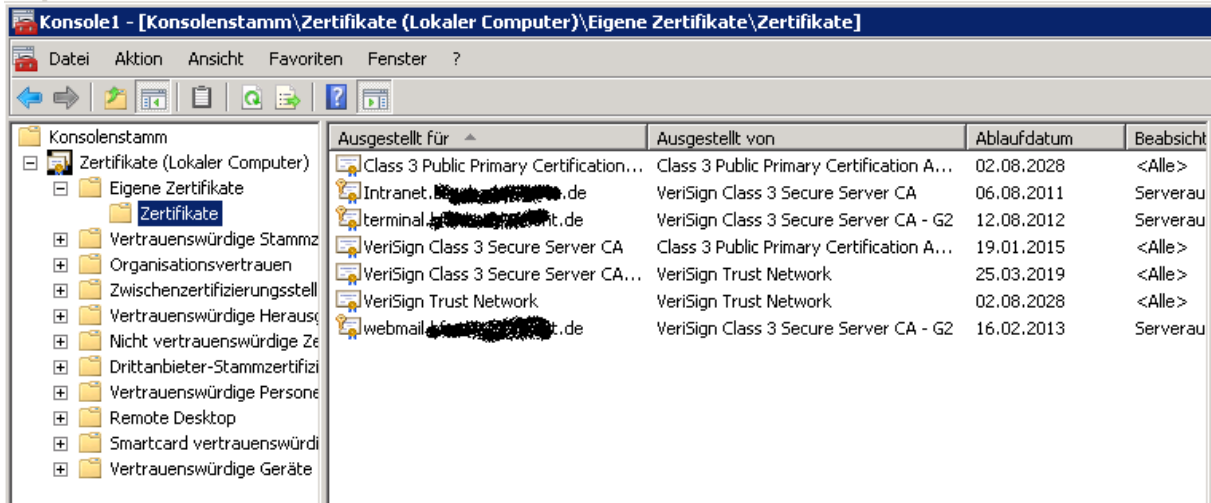


Auf Wiedersehen 😊

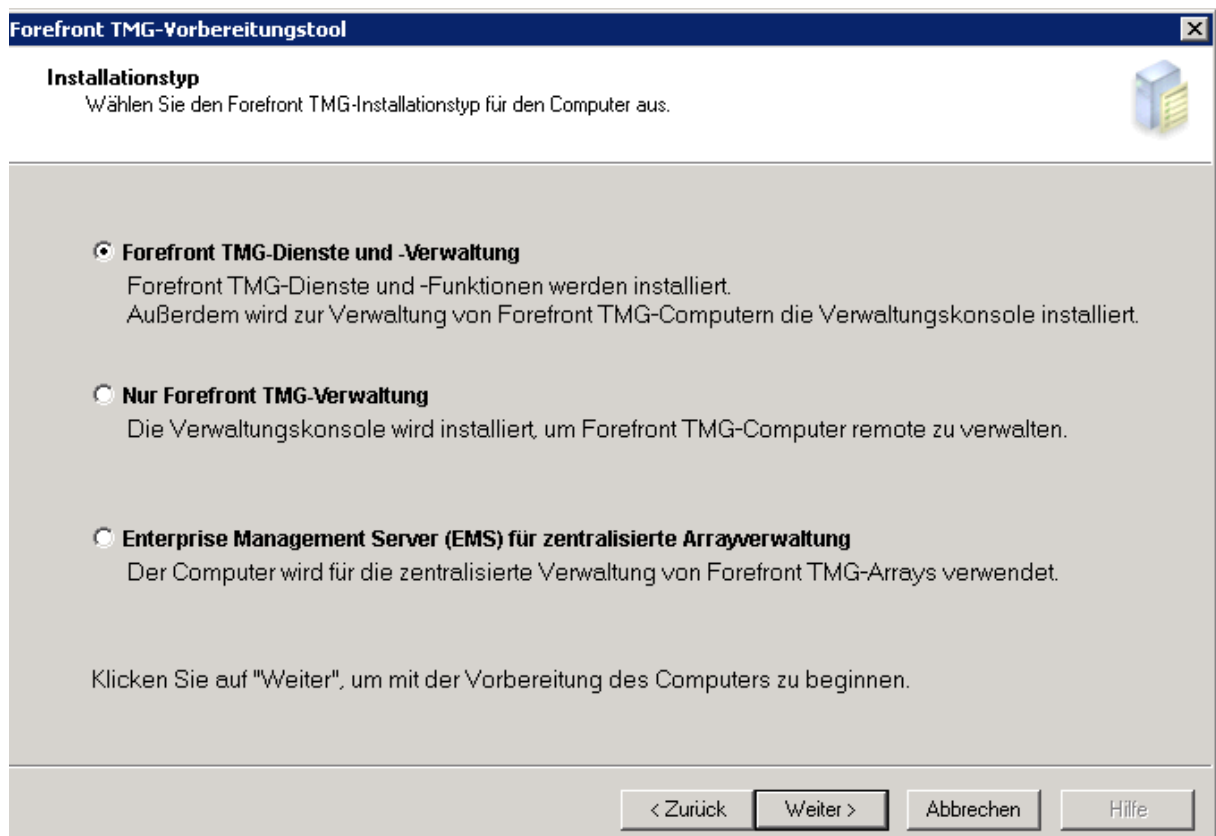


## TMG Node 1 Installation

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



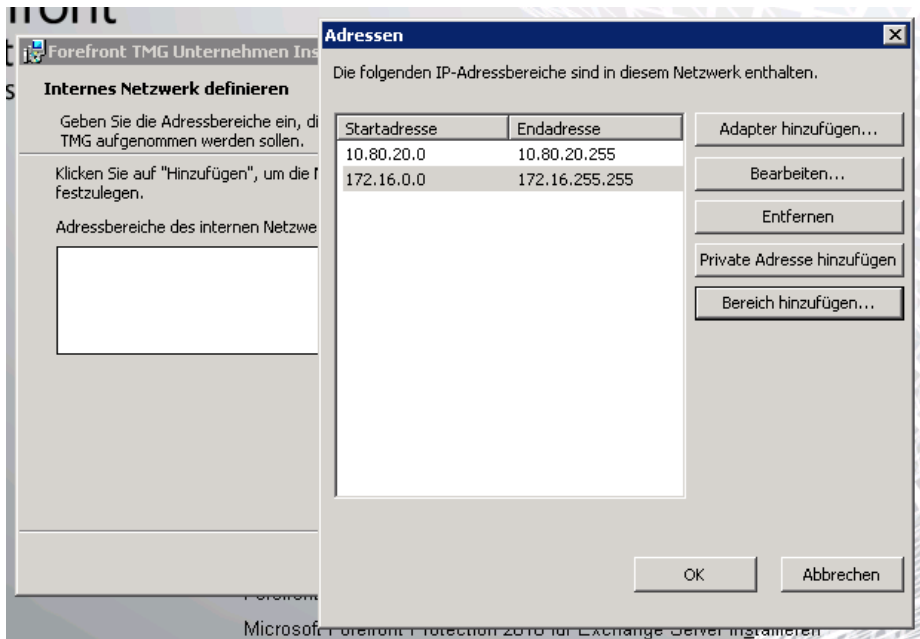
## TMG Vorbereitungstool



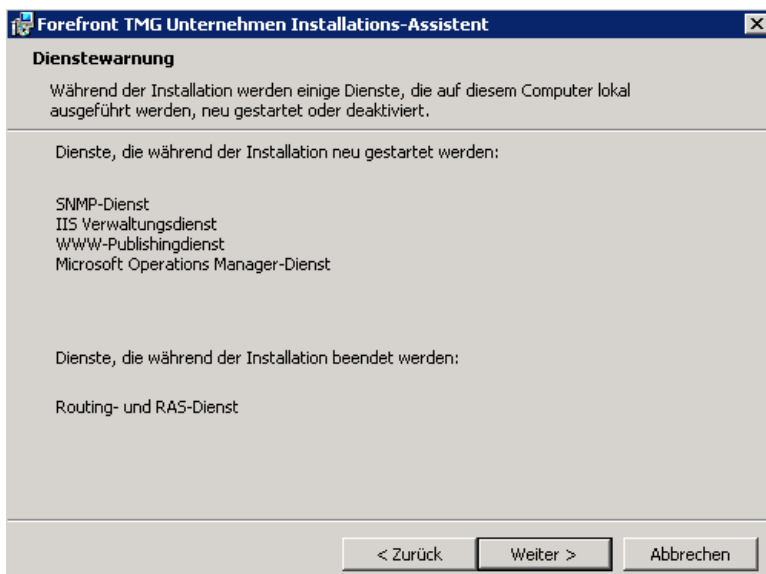


## TMG installieren

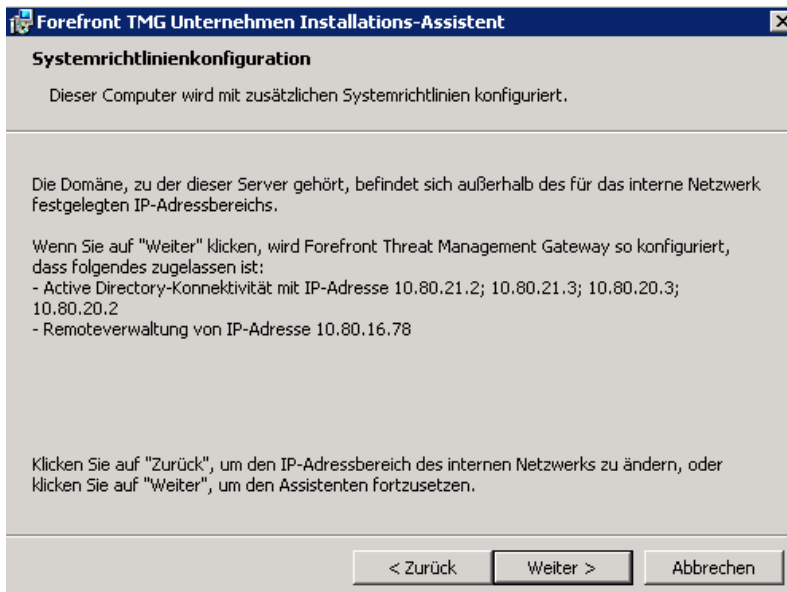
### Interne IP-Adressbereiche angeben



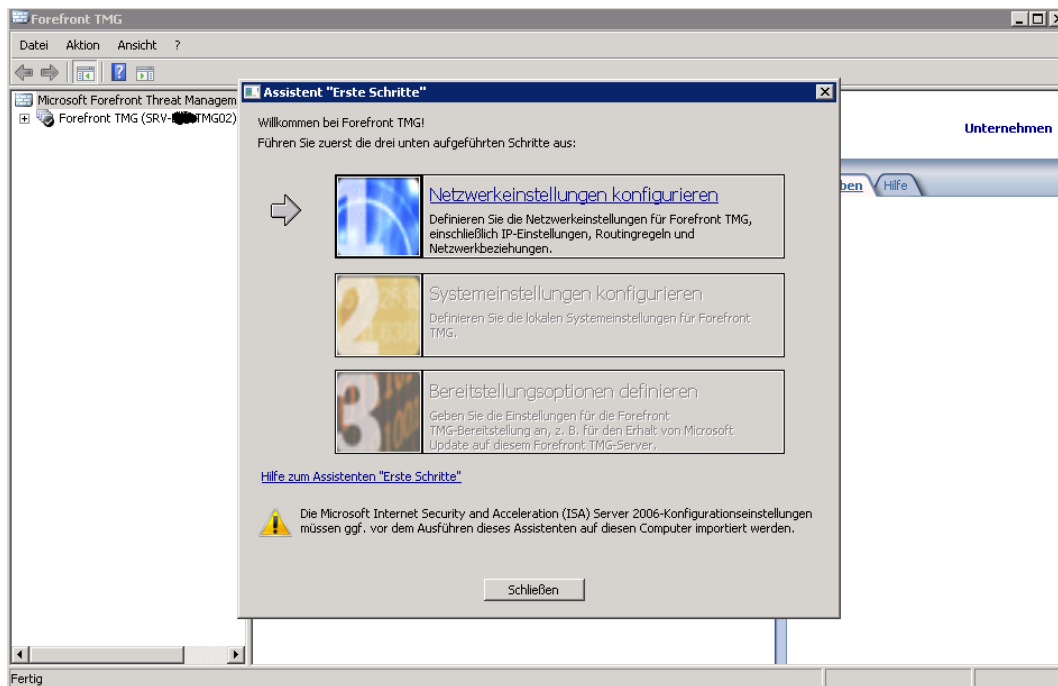
Während der Installation zu beendende Dienste, so sie denn installiert sind



Systemrichtlinienkonfiguration fuer AD-Zugriff und Remoteverwaltung (spaeter anpassen)



Nach erfolgter Installation TMG Erstinstallationswizard ausfuehren



Domaenenmitgliedschaft, Netzwerkkartenkonfiguration usw.

**Erste Schritte - Bereitstellungs-Assistent**


**Einstellungen für Schutzfeatures von Forefront TMG**  
 Auf dieser Seite können Sie Lizenzen aktivieren, die für Aktualisierungen und zum Aktivieren des Forefront TMG-Schutzmechanismus benötigt werden.

Netzwerküberprüfungssystem (NIS)  
 Lizenz:

[Was ist NIS?](#)

Webschutz  
 Lizenz:   
 Schlüssel:  Ablaufdatum:

Malwareüberprüfung aktivieren  
 URL-Filterung aktivieren

 Mit der URL-Filterungsfunktion wird die URL-Kategorisierung vom Microsoft-Zuverlässigkeitsdienst abgefragt. Die vollständige URL-Zeichenfolge wird über eine sichere Verbindung an den Dienst gesendet.

[Informationen zur Aktualisierung von Lizenzverträgen](#)  
[Datenschutzerklärung anzeigen](#)

< Zurück Weiter > Abbrechen

**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.

**Erste Schritte - Bereitstellungs-Assistent**

**Microsoft-Berichterstattungsdienst für Telemetrie**  
 Wählen Sie eine Teilnahmeebene für die telemetrische Berichterstattung von Microsoft aus.

Wenn Sie sich für die Teilnahme an der telemetrischen Berichterstattung von Microsoft entscheiden, werden Informationen über Malware und andere Angriffe auf Ihr Netzwerk an Microsoft übermittelt. Mithilfe dieser Informationen kann Microsoft die Forefront TMG-Funktionen zum Ermitteln von Angriffsmustern und zur Abwehr von Risiken verbessern. In einigen Fällen werden möglicherweise unbeabsichtigt persönliche Informationen gesendet. Microsoft verwendet diese Informationen jedoch nicht, um Sie zu identifizieren oder zu kontaktieren.

Wählen Sie aus, wie Sie sich beteiligen möchten:

Standard  
 Grundlegende Informationen zu potenziellen Bedrohungen, einschließlich Typ, Ursache und unternommener Gegenmaßnahmen, werden an Microsoft gesendet.

Erweitert  
 Neben den grundlegenden Informationen werden genauere Informationen zu potenziellen Bedrohungen, einschließlich Proben des Datenverkehrs und vollständiger URL-Zeichenfolgen, an Microsoft gesendet. Anhand dieser zusätzlichen Informationen kann Microsoft Bedrohungen besser analysieren und abwehren.

Keine. Es werden keine Informationen an Microsoft gesendet.

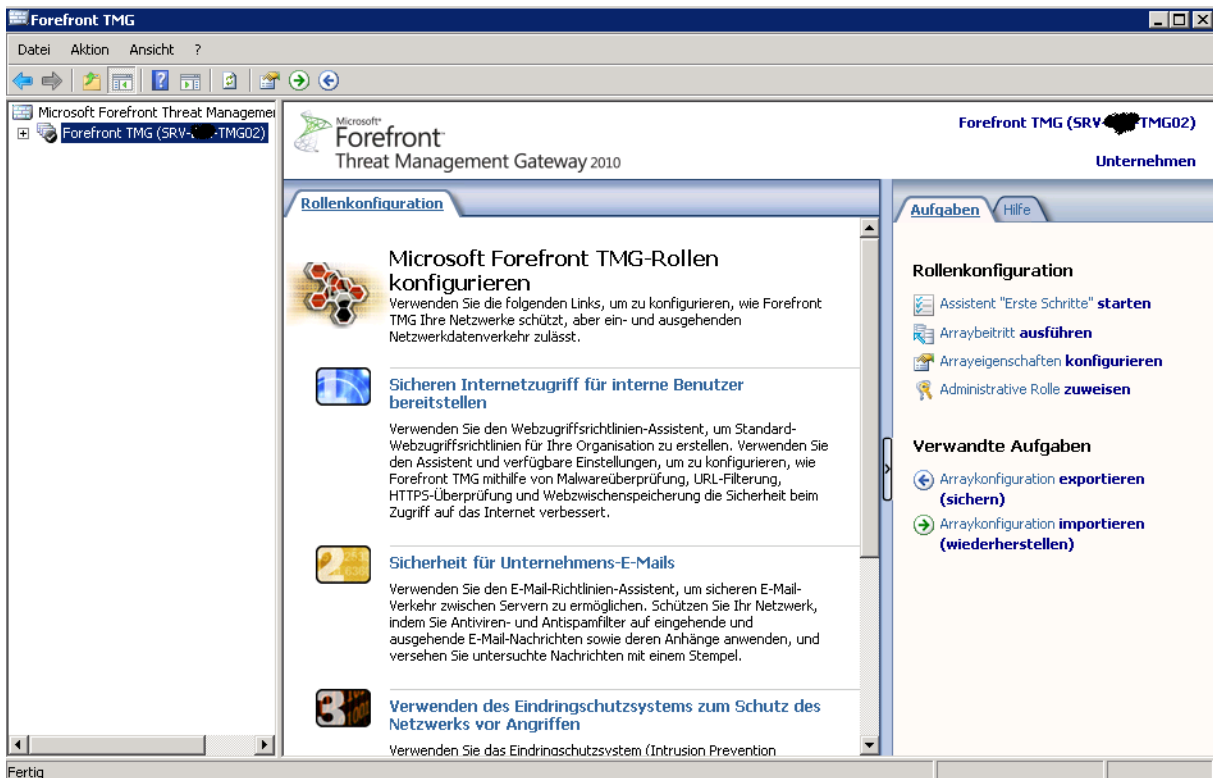
[Datenschutzerklärung anzeigen](#)

< Zurück Weiter > Abbrechen

Assistenten fuer Webzugriff nicht ausfuehren



## Arraybeitritt ausführen



## EMS Beitritt

**Arraybeitritts-Assistent** [X]

**Arraymitgliedschaftstyp**  
Wählen Sie den Typ des Arrays aus, dem dieser Forefront TMG-Server beitreten soll.

Arrayoptionen:

- Beitritt zu einem Array, das von einem EMS verwaltet wird.
- Beitritt zu einem eigenständigen Array, das von einem ausgewählten Arraymitglied (dem Array-Manager) verwaltet wird.

< Zurück   Weiter >   Abbrechen

## EMS Server angeben

**Arraybeitritts-Assistent** [X]

**Details zum EMS (Enterprise Management Server)**  
Wählen Sie den EMS aus, und geben Sie das Benutzerkonto an, mit dem eine Verbindung zum ausgewählten Server hergestellt werden soll.

Vollqualifizierter Domänenname (FQDN) des EMS:

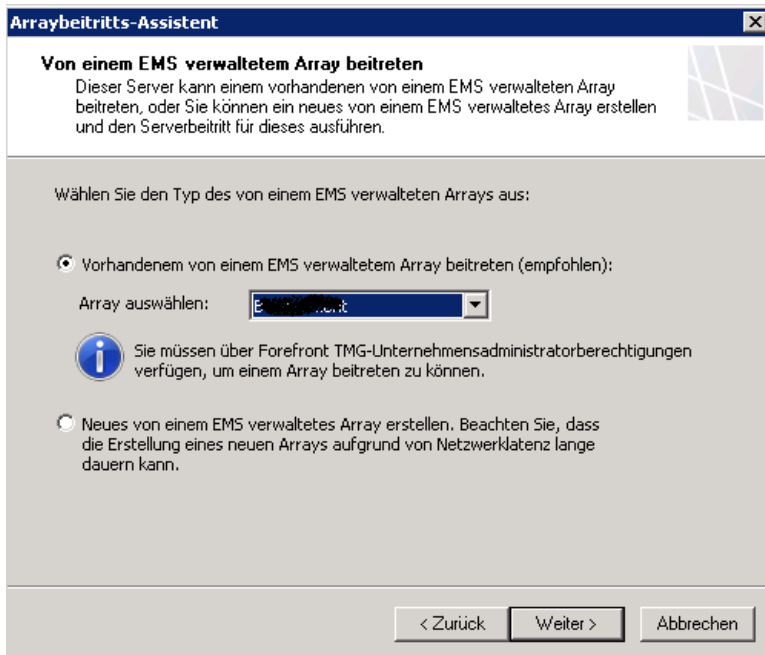
SRV-EMS01.local   Durchsuchen...

Benutzerkonto mit geeigneten Rechten für die Verbindung mit dem EMS

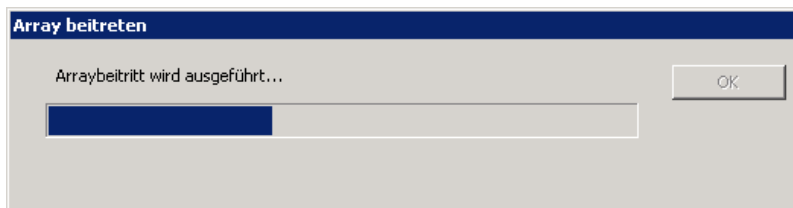
- Über die Anmeldeinformationen des angemeldeten Benutzers verbinden
- Über dieses Konto verbinden:  
Benutzername: \_\_\_\_\_  
Kennwort: \_\_\_\_\_

< Zurück   Weiter >   Abbrechen

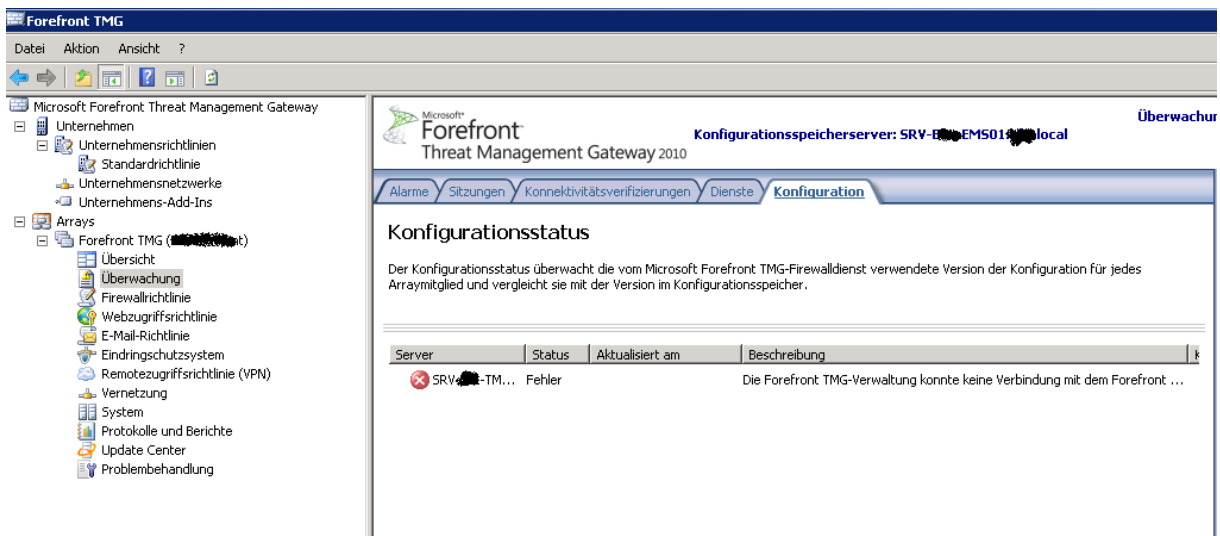
## EMS Array waehlen



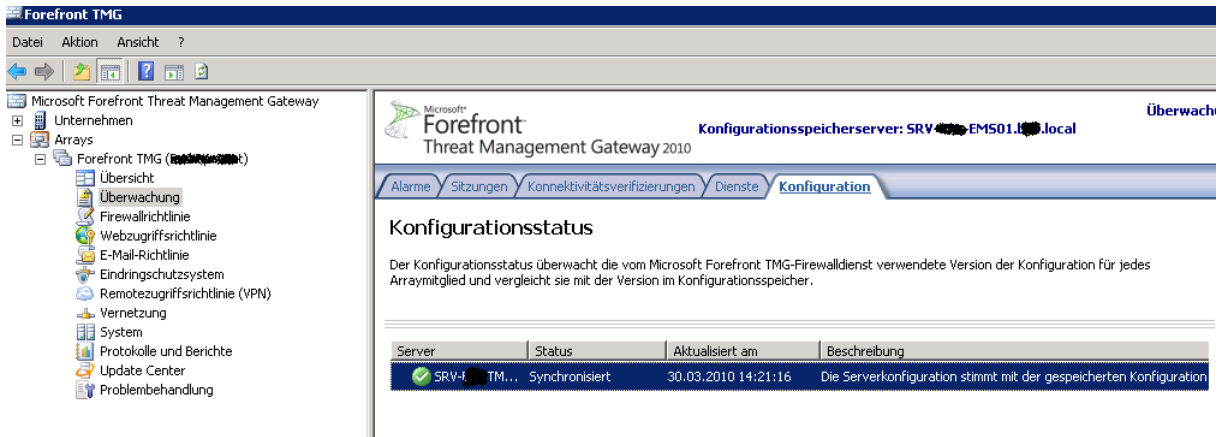
Ab geht es



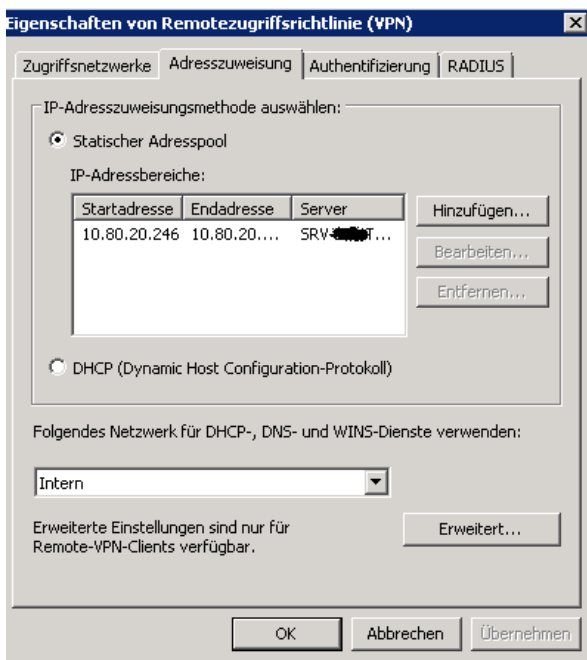
Da taucht schon was auf dem EMS auf



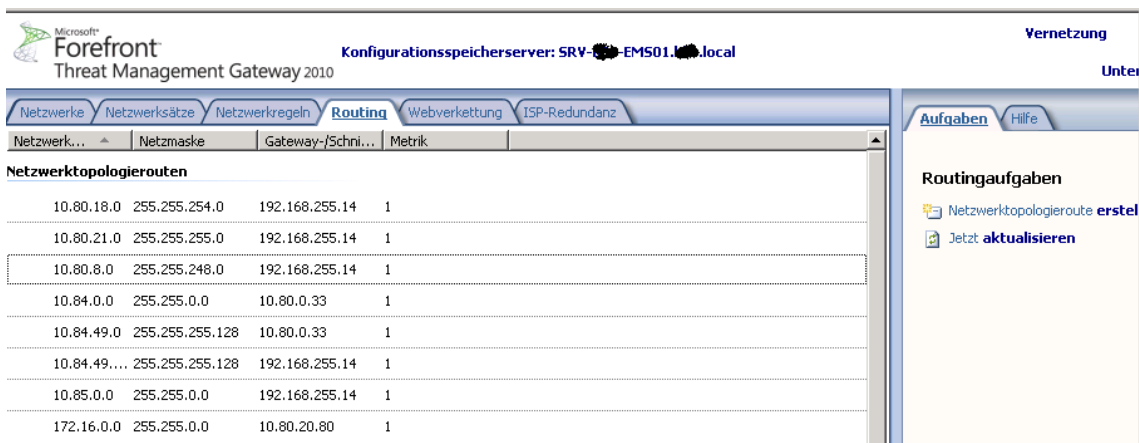
Alles schoen. Dauert etwas?!



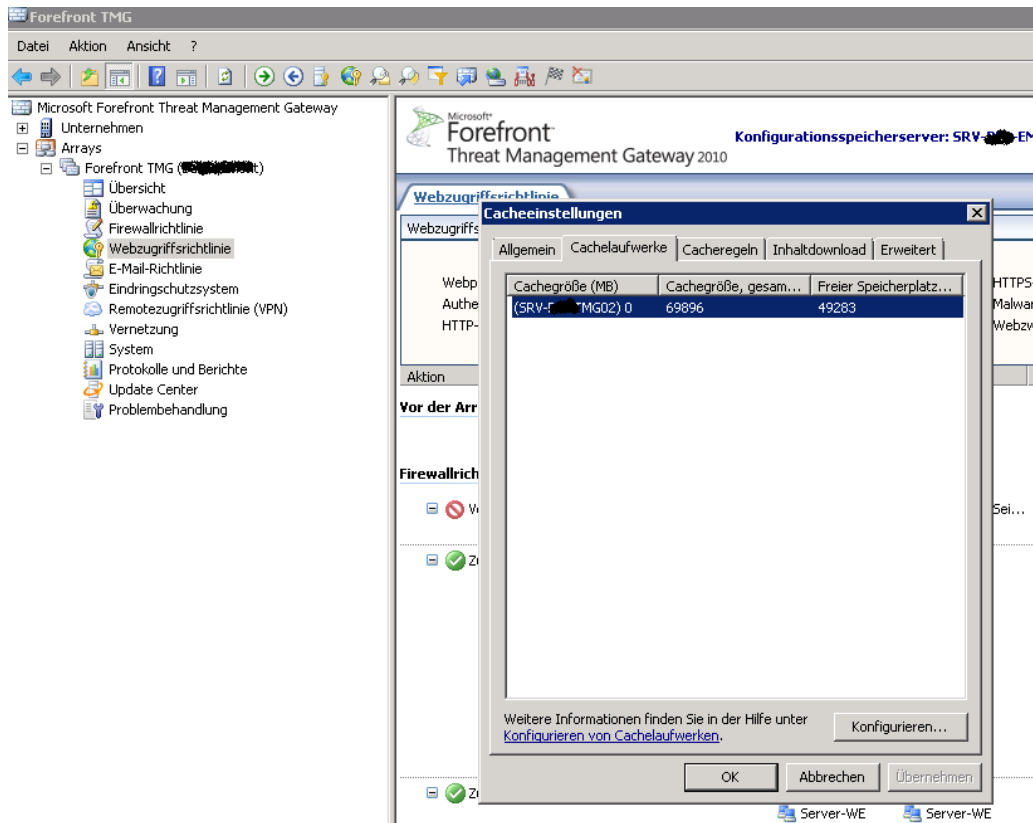
## VPN Konfiguration



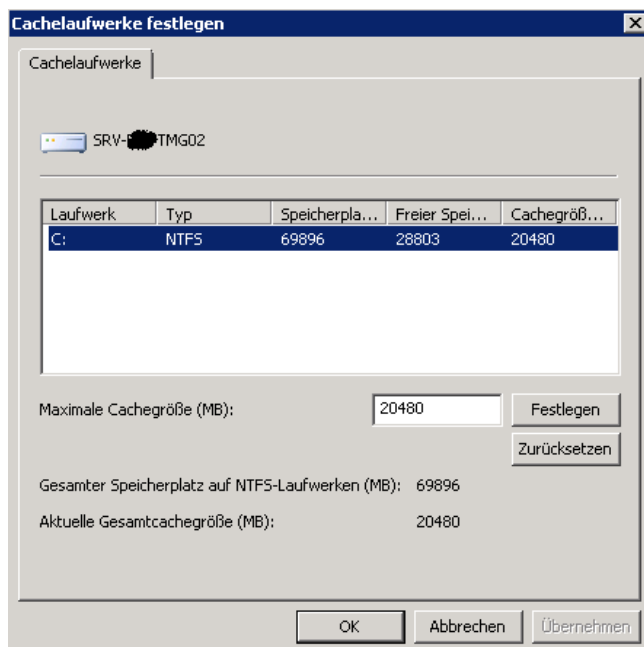
Routen adden – jetzt sehr schoen im EMS gespeichert und ueber die GUI konfigurierbar.



## Cache Konfiguration

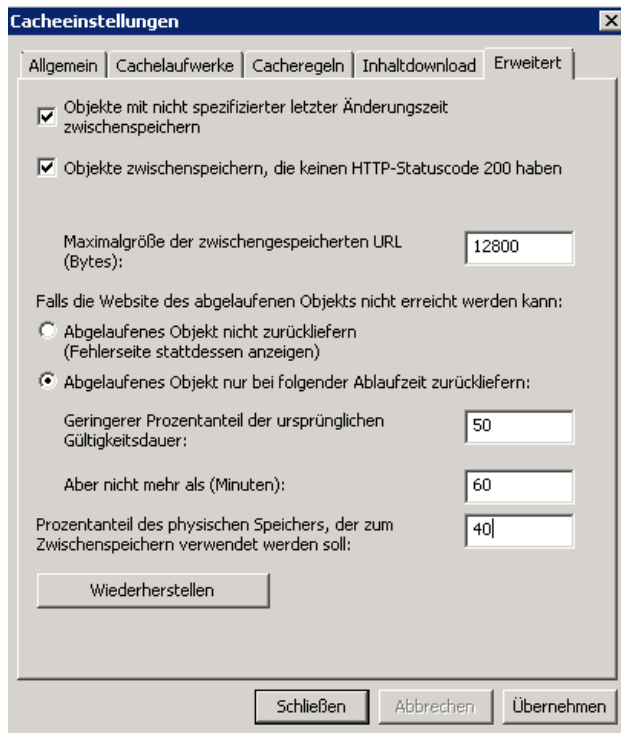


## Cachegrösse festlegen



## Cachesize auf 40% vergrößern



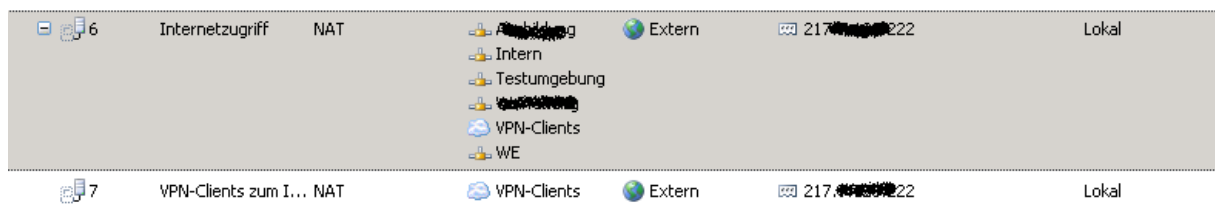


Konfigurationsänderung übernehmen und Dienste neu starten

Nach den vorgenommenen Änderungen kann der TMG Server in Produktionsbetrieb genommen werden und die Funktionalität 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:



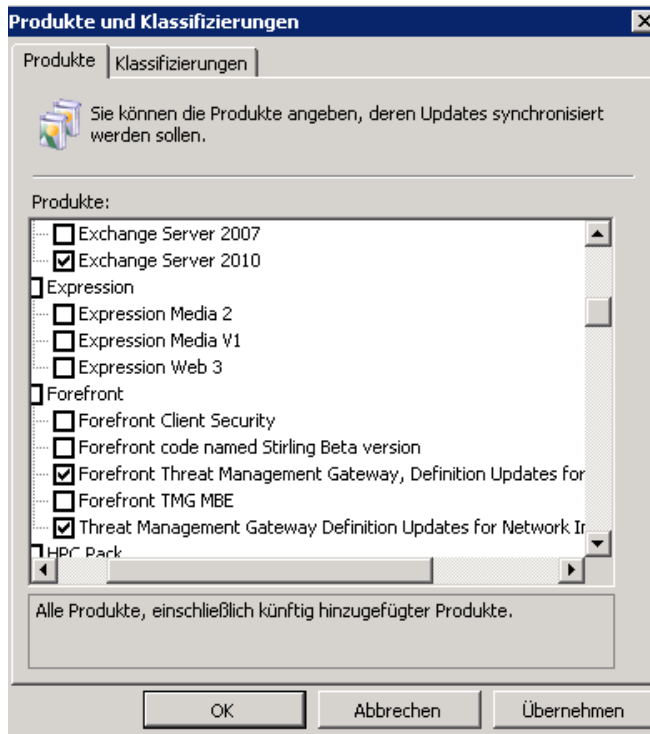
Das scheint bei Design so zu sein und kein TMG Problem:

<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/>

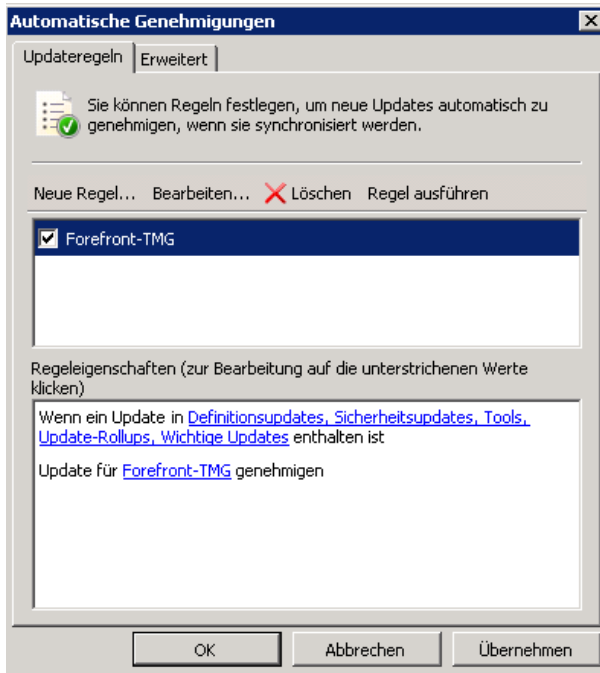
## WSUS fuer Updates verwenden



## 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

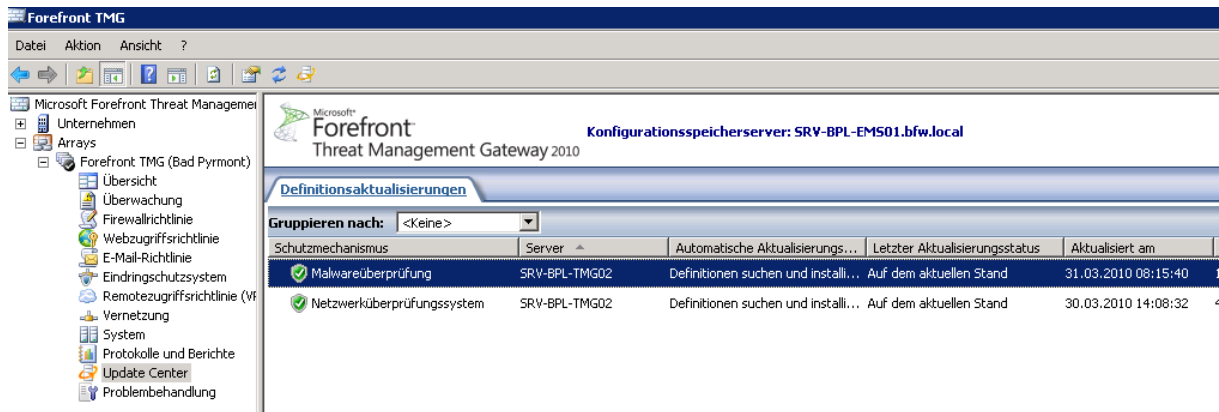
##### Administrative Vorlagen

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

##### Windows-Komponenten/Windows Update

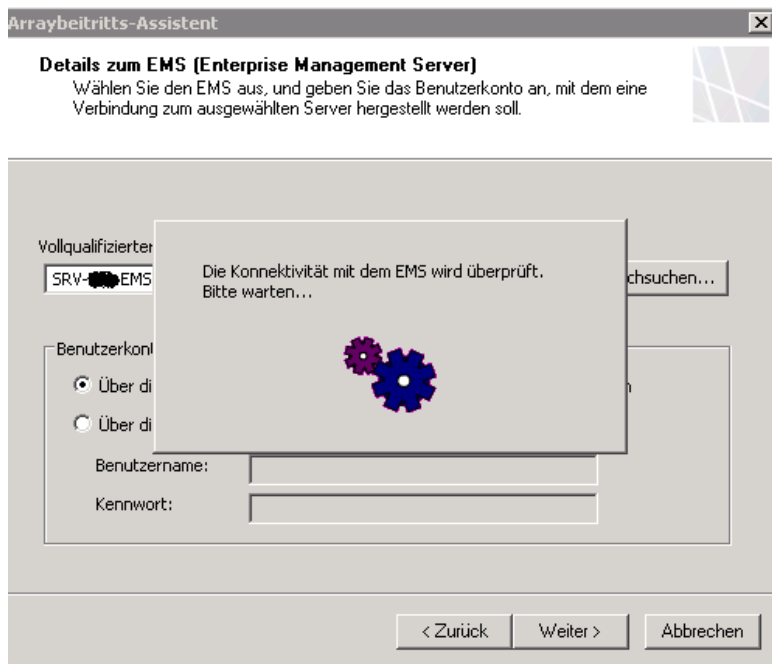
Richtlinie	Einstellung	Kommentar
Automatische Updates konfigurieren:	Aktiviert	
4 - Autom. Herunterladen und laut Zeitplan installieren		
Folgende Einstellungen sind nur erforderlich und gültig, wenn 4 ausgewählt wird.		
Geplanter Installationstag:	0 - Täglich	
Geplante Installationszeit:	03:00	
Richtlinie	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-tdm01.local
Intranetserver für die Statistik:		http://srv-tdm01.local
(Beispiel: http://IntranetUpd01)		
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

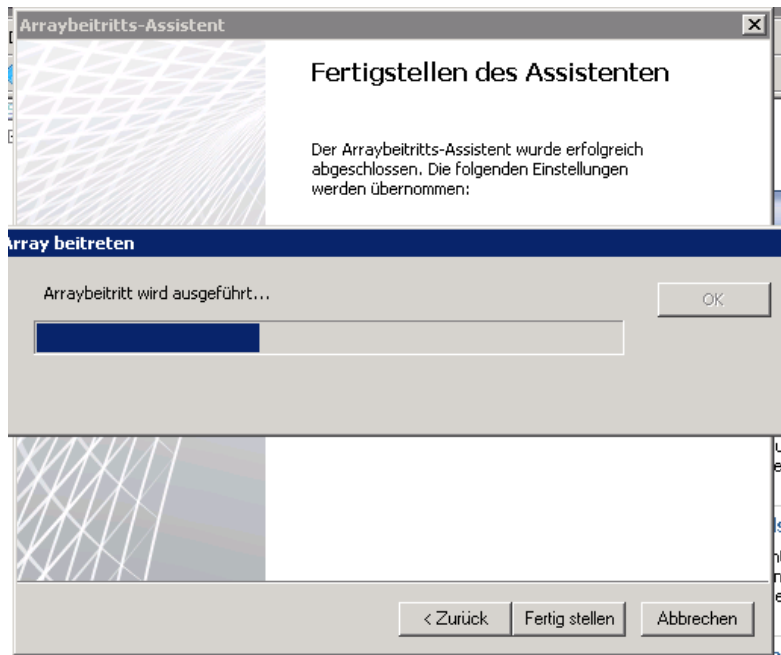


## Zweiten Forefront TMG Knoten installieren

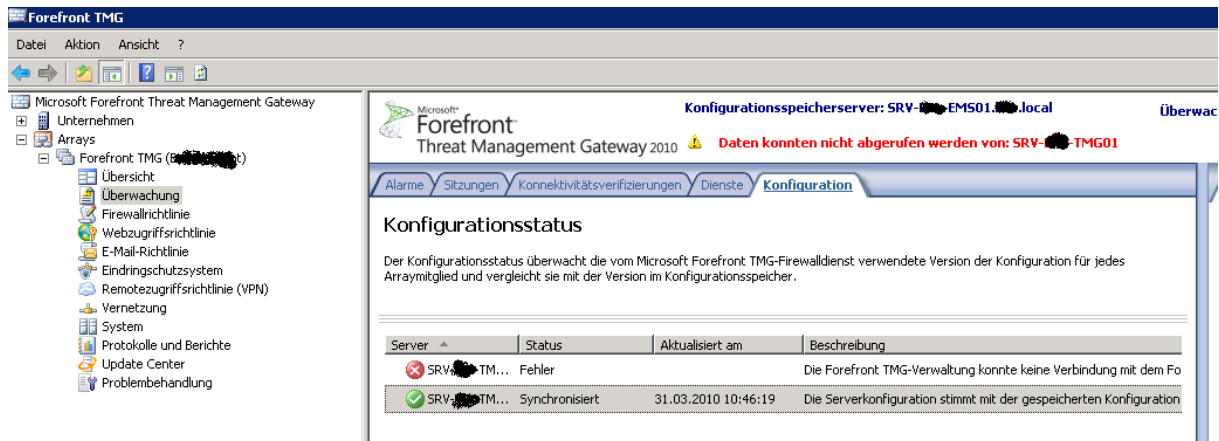
## Dem EMS beitreten



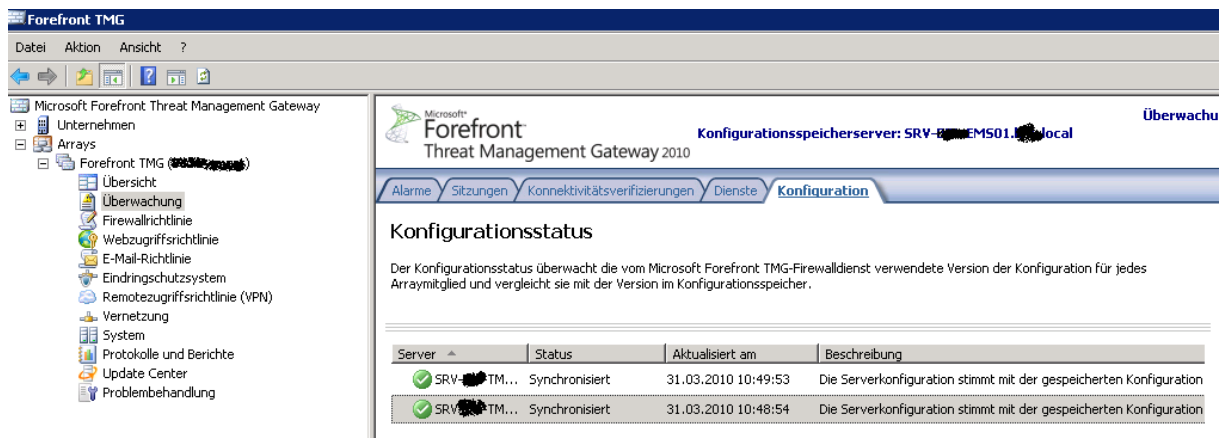
## Beitritt wird durchgeführt



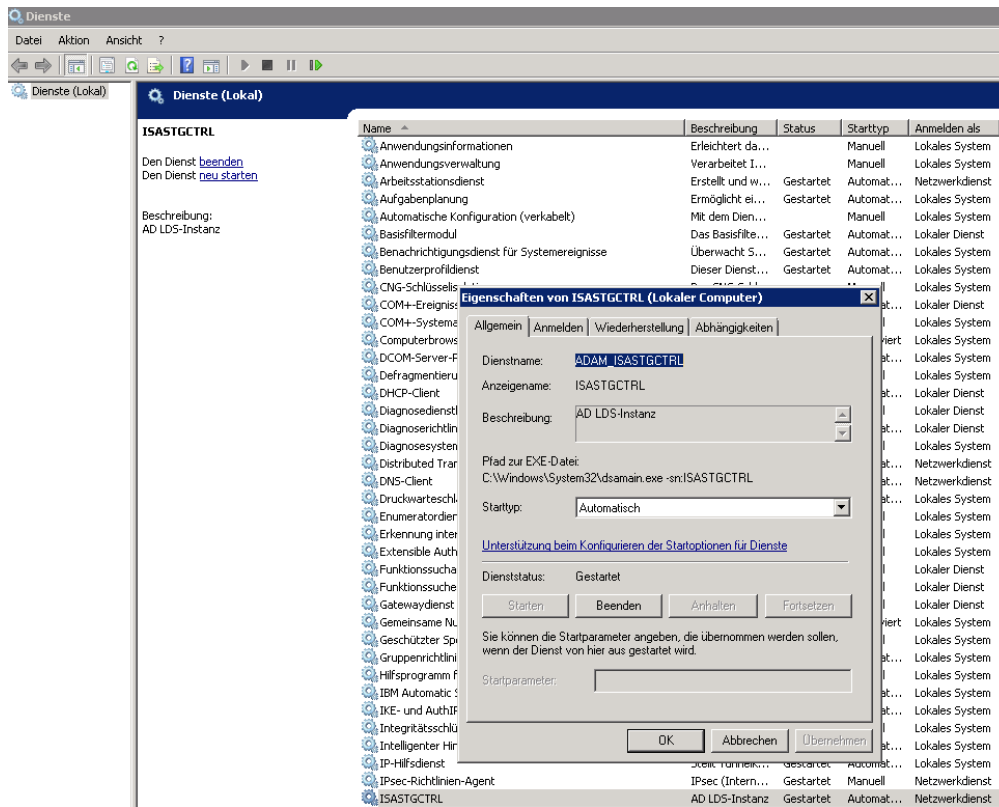
## So langsam tut sich was



## 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

Beschreibung: AD LDS-Instanz	Active Directory-Webdienste	Mit diesem Di...	Gestartet	Automat...	Lokales System
	Anmeldedienst	Unterstützt e...	Gestartet	Automat...	Lokales System
	Anmeldeinformationsverwaltung	Ermöglicht da...		Manuell	Lokales System
	Anschlussumleitung für Remotedesktop...	Ermöglicht di...	Gestartet	Manuell	Lokales System
	Anwendungserfahrung	Verarbeitet A...		Manuell	Lokales System
	Anwendungsidentität	Bestimmt und...		Manuell	Lokaler Dienst
	Anwendungsinformationen	Erleichtert da...	Gestartet	Manuell	Lokales System
	Anwendungsverwaltung	Verarbeitet I...		Manuell	Lokales System
	Arbeitsstations...				
	Aufgabenplanu...				
	Automatische K...				
	Basisfiltermodul				
	Benachrichtiger				
	Benutzerprofilid				
	CNG-Schlüsselis				
	COM+-Ereignis...				
	COM+-Systeme...				
	Computerbrows...				
	DCOM-Server-F...				
	Defragmentieru...				
	DHCP-Client				
	Diagnosedienstl				
	Diagnoserichtlin				
	Diagnosesystem				
	Distributed Trar				
	DNS-Client				
	Druckwarteschl.				
	Enumeratordien				
	Erkennung inter				
	Extensible Auth				
	Funktionssucha				
	Funktionssuche				
	Gatewaydienst				
	Gemeinsame N...				
	Geschützter Sp...				
	Gruppenrichtliniendienst	Von dem Dien...	Gestartet	Automat...	Lokales System
	Hilfsprogramm für spezielle Verwaltun...	Ermöglicht Ad...		Manuell	Lokales System
	IBM Remote Supervisor Adapter II		Gestartet	Automat...	Lokales System
	IKE- und AuthIP IPsec-Schlüsselerstellu...	Die IKEEXT-Di...	Gestartet	Automat...	Lokales System
	Integritätsschlüssel- und Zertifikatverw...	Stellt ein X.5...		Manuell	Lokales System
	Intelligenter Hintergrundübertragungsdi...	Überträgt Da...	Gestartet	Manuell	Lokales System
	IP-Hilfsdienst	Stellt Tunnelk...	Gestartet	Automat...	Lokales System
	IPsec-Richtlinien-Agent	IPsec (Intern...	Gestartet	Manuell	Netzwerkdienst
	ISASTGCTRL	AD LDS-Instanz	Deaktiviert		Netzwerkdienst

**Eigenschaften von ISASTGCTRL (Lokaler Computer)**

Allgemein | Anmelden | Wiederherstellung | Abhängigkeiten

Dienstname: **ADAM ISASTGCTRL**

Anzeigename: ISASTGCTRL

Beschreibung: AD LDS-Instanz

Pfad zur EXE-Datei: C:\Windows\System32\dsamain.exe -sn:ISASTGCTRL

Starttyp: Deaktiviert

[Unterstützung beim Konfigurieren der Startoptionen für Dienste](#)

Dienststatus: Beendet

[Starten] [Beenden] [Anhalten] [Fortsetzen]

Sie können die Startparameter angeben, die übernommen werden sollen, wenn der Dienst von hier aus gestartet wird.

Startparameter:

[OK] [Abbrechen] [Übernehmen]

## EMS anpassen fuer TMG Node Zugriff

**Eigenschaften von Konfigurationsspeicherserver für das Unterne...**

Allgemein

Name: Konfigurationsspeicherserver für das Unternehmen

Regeln, die Domännennamensätze verwenden, werden eventuell nicht wie erwartet angewendet, falls DNS nicht richtig konfiguriert ist.

In diesem Satz enthaltene Domännennamen:

SRV-EM501.local

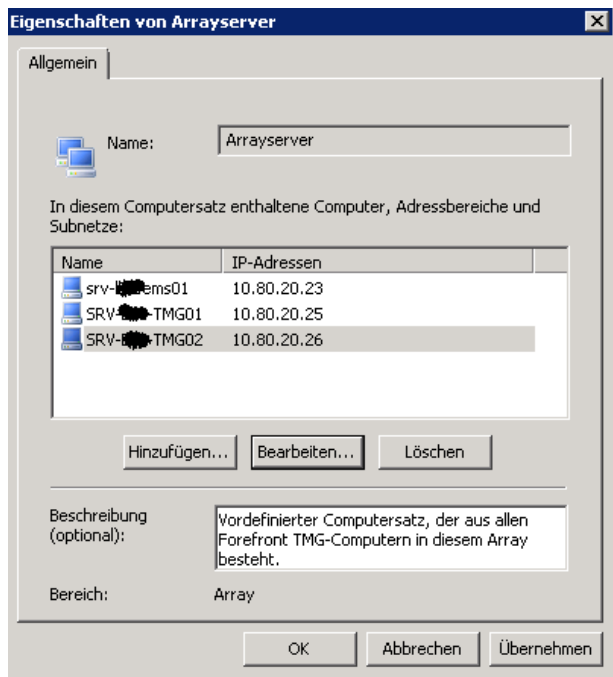
[Hinzufügen] [Umbenennen] [Löschen]

Beschreibung (optional): Vordefinierter Domännennamensatz für die Konfigurationsspeicherserver, die von diesem Forefront TMG-Computer verwendet werden.

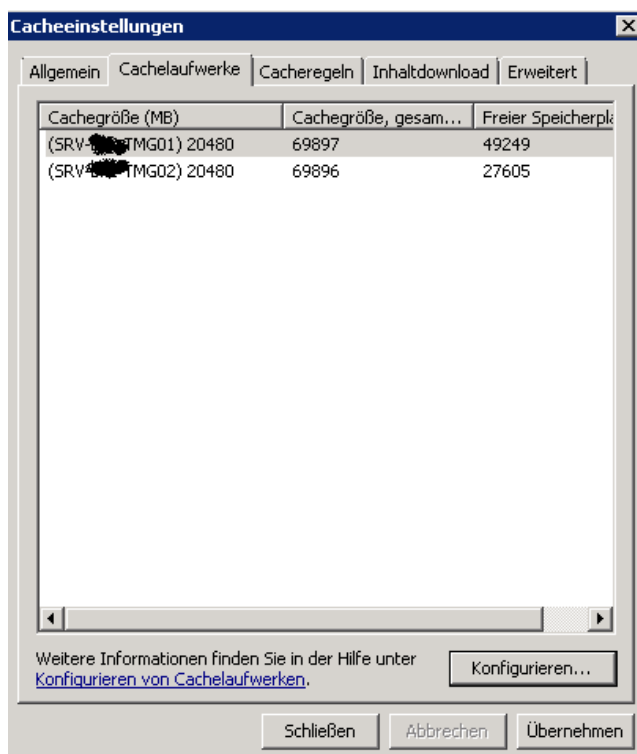
Bereich: Array

[OK] [Abbrechen] [Übernehmen]

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

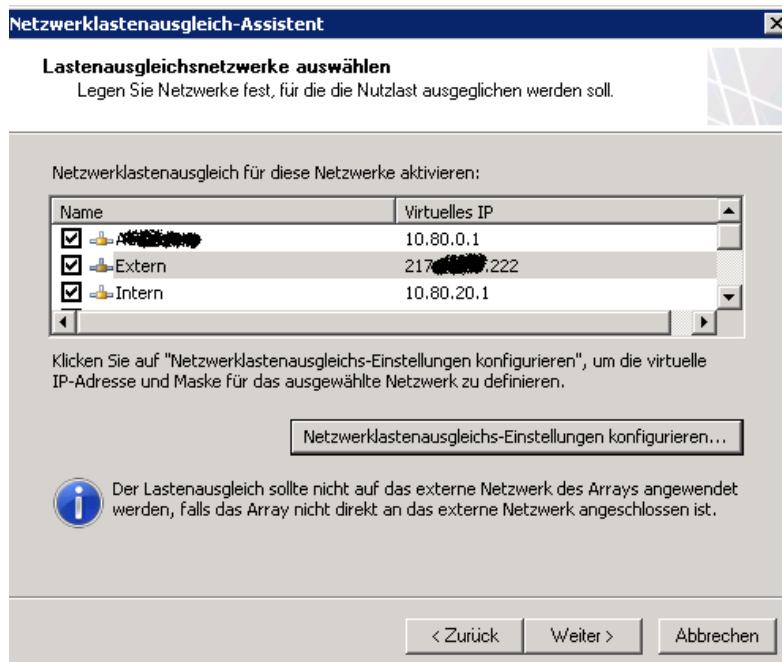


Cache auf dem zweiten Knoten aktivieren

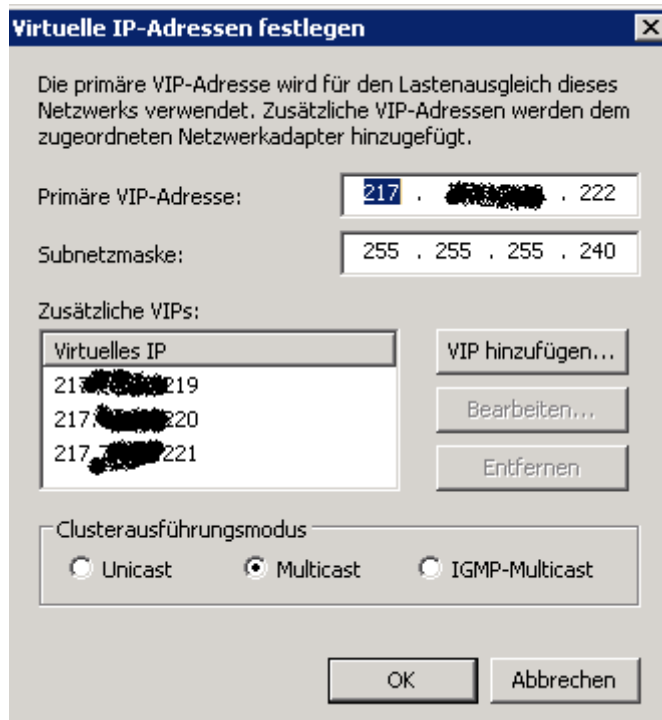




## NLB aktivieren



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



## Dienste neu starten, Kaffee trinken oder rauchen und immer beten

Microsoft Forefront Threat Management Gateway 2010

Konfigurationsspeicherserver: SRV-...-EMS01-...local

Übernehmen Verwerfen

Klicken Sie auf "Übernehmen", um Änderungen zu speichern und die Konfiguration zu übernehmen.

Netzwerke Netzwerksätze **Netzwerkregeln** Netzwerkadapter Routing Webverkettung TSP-Redundanz

Reihenfolge Name Beziehung Quellnetzwerke Zielnetzwerke NAT-Adressen Beschreibung

**Lokale Netzwerkregeln**

1	Lokaler Hostzugriff	Route
2	...	Route
3	A...	Route
4	...	Route
5	VPN-Clients zum I...	Route
6	Internetzugriff	NAT
7	VPN-Clients zum I...	NAT
8	BP <-> WE	Route

**Unternehmensnetzwerkregeln**

**Forefront TMG-Warnung**

Änderungen werden erst wirksam, nachdem folgende Dienste neu gestartet wurden:

Array	Dienst
...	Microsoft Forefront TMG...

Änderungen speichern, aber Dienste nicht neu starten  
Die Änderungen werden erst wirksam, nachdem Sie die Dienste manuell neu gestartet haben.

Änderungen speichern und Dienste neu starten  
Änderungen werden nach Neustart der Dienste angewendet. Dieser Vorgang kann einige Minuten dauern. Alle beendeten Dienste müssen manuell gestartet werden.

OK Abbrechen

## NLB Manager Ansicht

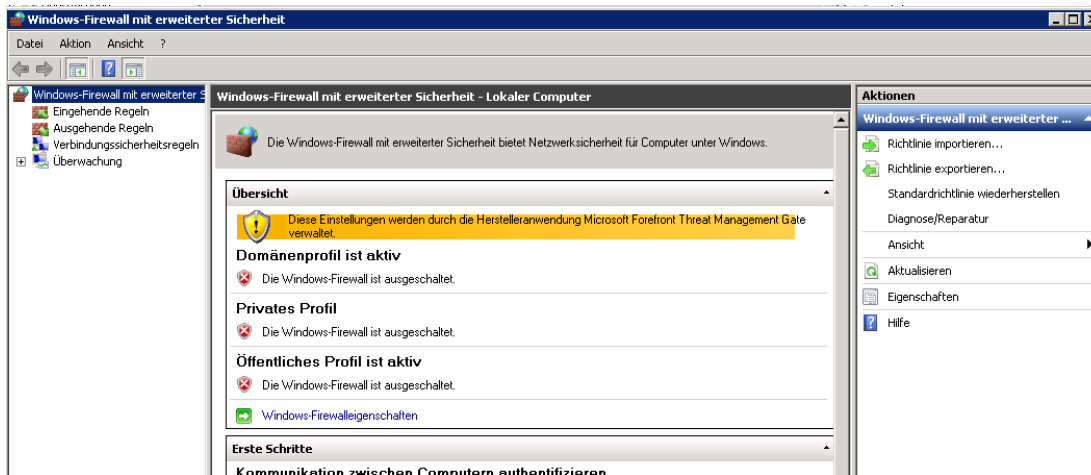
Netzwerklastenausgleich-Manager

Clusterkonfiguration für alle bekannten NLB-Cluster

Clustername	Cluster-IP-Adresse	Cluster-IP-Subnetzmaske	Clustermodus
...	10.80.0.1	255.255.248.0	Multicast
Extern	217.70.0.22	255.255.255.240	Multicast
...	10.80.16.1	255.255.254.0	Multicast
Intern	10.80.20.1	255.255.255.0	Multicast
...	192.168.255.11	255.255.255.248	Multicast

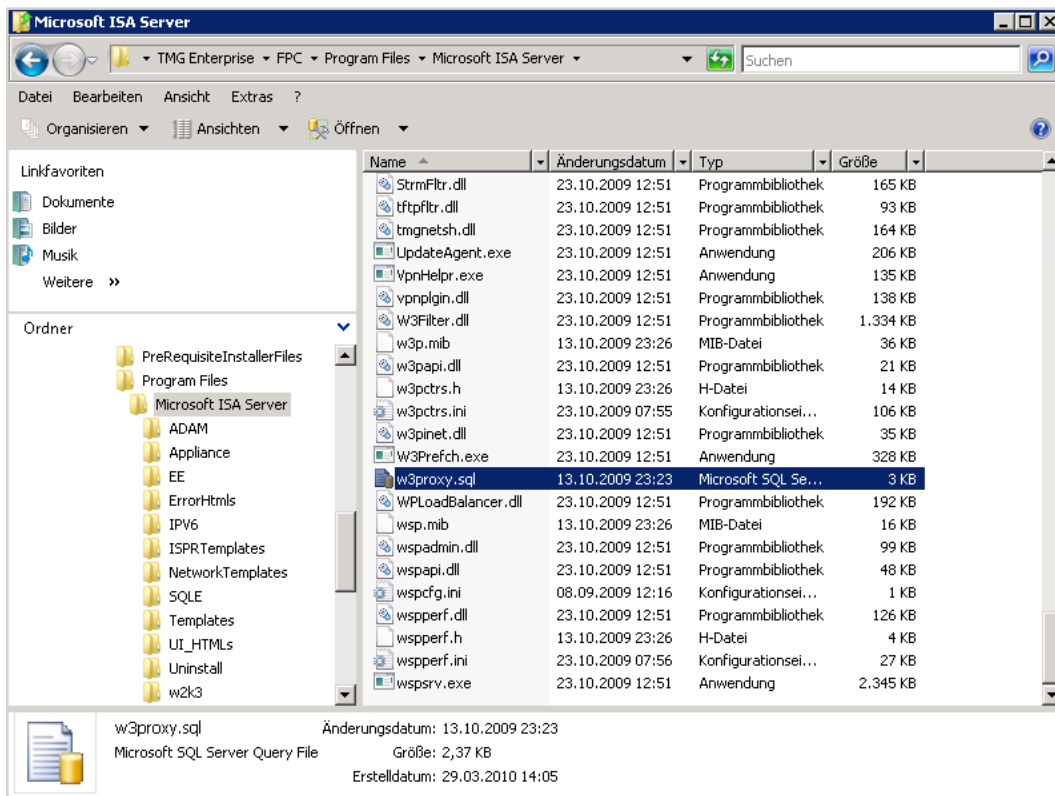
Protok...	Datum	Zeit	Cluster	Host	Beschreibung
0002	31.03.2010	13:19:01			Lokal gebundene Instanzen werden geladen
0003	31.03.2010	13:19:02			Konfigurationsinformationen von Host "SRV-...-TMG01-...local" für Cluster "10.80.0.1" werden ...
0004	31.03.2010	13:19:10			Konfigurationsinformationen von Host "SRV-...-TMG02-...local" für Cluster "10.80.0.1" werden ...
0005	31.03.2010	13:19:10			Konfigurationsinformationen von Host "SRV-...-TMG01-...local" für Cluster "217.70.0.22" werden...
0006	31.03.2010	13:19:16			Konfigurationsinformationen von Host "SRV-...-TMG02-...local" für Cluster "217.70.0.22" wer...
0007	31.03.2010	13:19:17			Konfigurationsinformationen von Host "SRV-...-TMG01-...local" für Cluster "10.80.16.1" werden...
0008	31.03.2010	13:19:24			Konfigurationsinformationen von Host "SRV-...-TMG02-...local" für Cluster "10.80.16.1" werden...
0009	31.03.2010	13:19:24			Konfigurationsinformationen von Host "SRV-...-TMG01-...local" für Cluster "10.80.20.1" werden...
0010	31.03.2010	13:19:31			Konfigurationsinformationen von Host "SRV-...-TMG02-...local" für Cluster "10.80.20.1" werden...
0011	31.03.2010	13:19:32			Konfigurationsinformationen von Host "SRV-...-TMG01-...local" für Cluster "192.168.255.11" we...
0012	31.03.2010	13:19:38			Konfigurationsinformationen von Host "SRV-...-TMG02-...local" für Cluster "192.168.255.11" we...

## Windows Firewall wird von TMG verwaltet

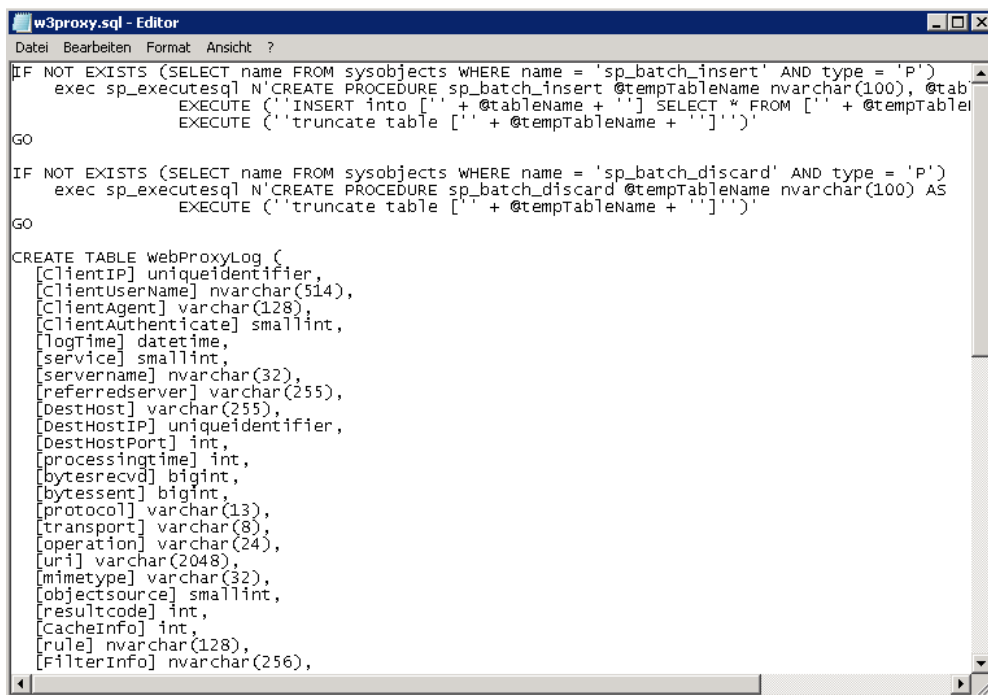


## SQL Server Logging einstellen

## Skripte lokalisieren



## Inhalt

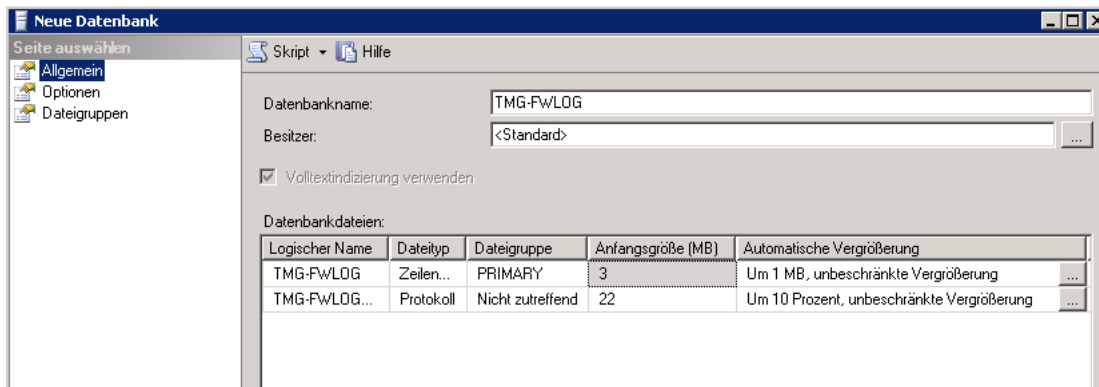


```
IF NOT EXISTS (SELECT name FROM sysobjects WHERE name = 'sp_batch_insert' AND type = 'P')
    exec sp_executesql N'CREATE PROCEDURE sp_batch_insert @tempTableName nvarchar(100), @tab
        EXECUTE ('INSERT into [' + @tableName + '] SELECT * FROM [' + @tempTable
        EXECUTE ('truncate table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

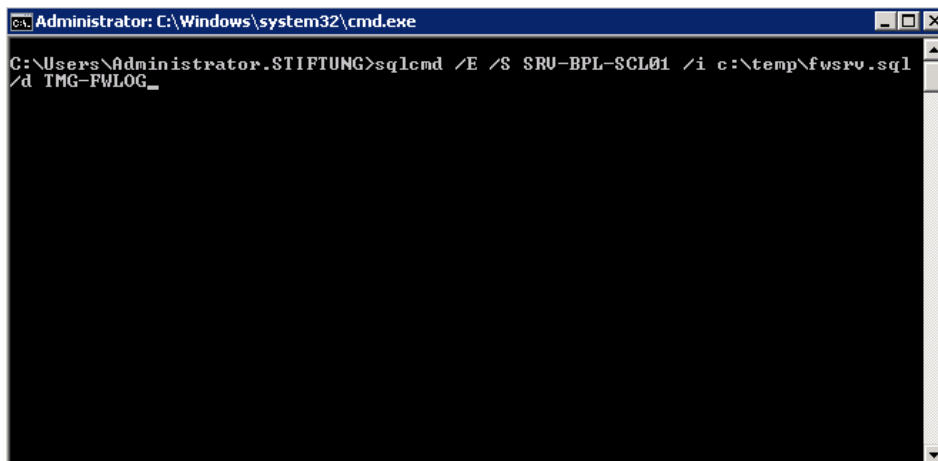
IF NOT EXISTS (SELECT name FROM sysobjects WHERE name = 'sp_batch_discard' AND type = 'P')
    exec sp_executesql N'CREATE PROCEDURE sp_batch_discard @tempTableName nvarchar(100) AS
        EXECUTE ('truncate table [' + @tempTableName + ']')'
GO

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),
    [objectsouce] 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



```
C:\Users\Administrator.STIFTUNG>sqlcmd /E /S SRU-BPL-SCL01 /i c:\temp\fwsvr.sql
/d TMG-FWLOG_
```

## Oder per Management Studio

```
SQLQuery1.sql...trator (116))*
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), @table
        EXECUTE ('INSERT into [' + @tableName + '] SELECT * FROM [' + @tempTableName + '
        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 FirewallLog (
    [servername] nvarchar(128),
    [logTime] datetime,
    [protocol] varchar(32),
    [SourceIP] uniqueidentifier,
    [SourcePort] int,
    [DestinationIP] uniqueidentifier,
    [DestinationPort] int,
```

Meldungen  
Befehl(e) wurde(n) erfolgreich abgeschlossen.

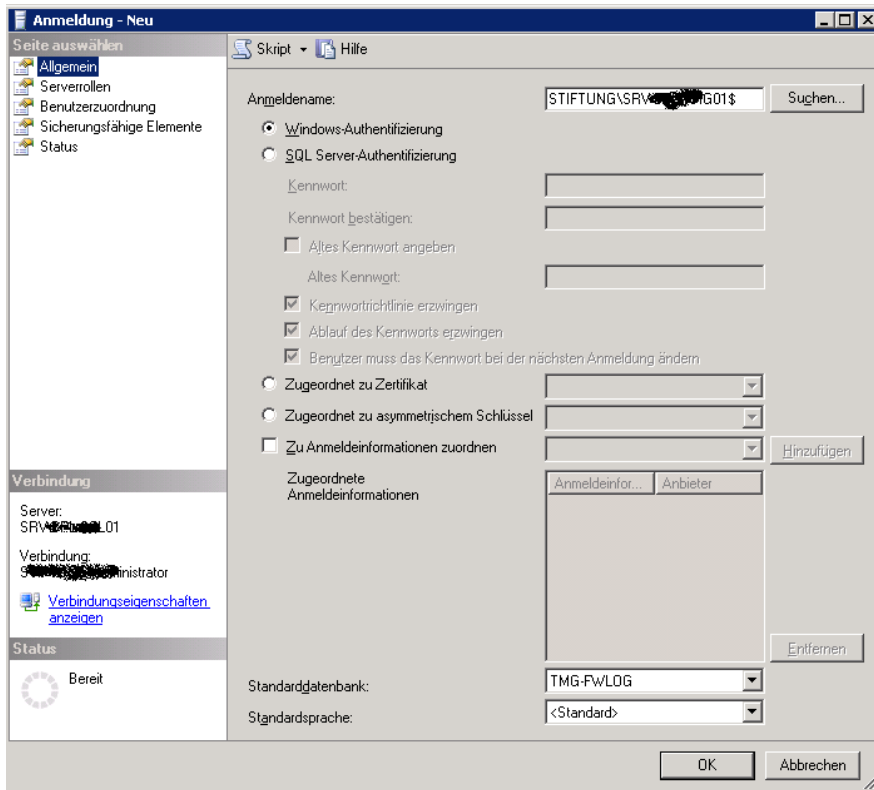
Das gleiche auch nochmal fuer das Webproxy Logging

DB anlegen

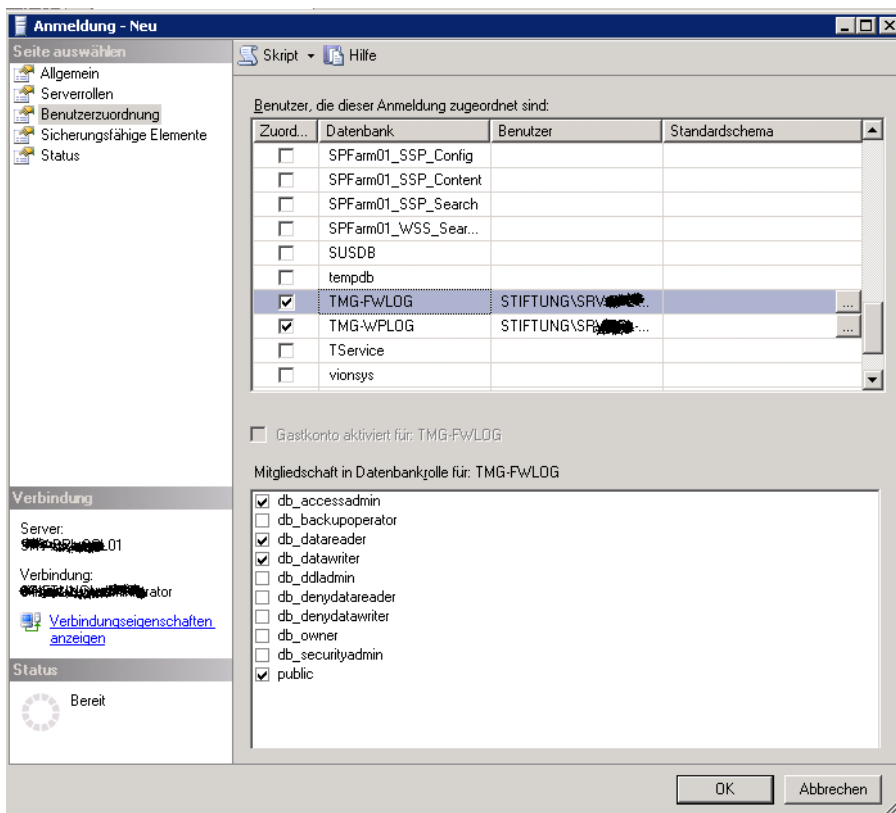
DB mit Tabellen fuehlen

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator.STIFTUNG>sqlcmd /E /S SRU-BPL-SCL01 /i c:\temp\w3proxy.sql
 /d TMG-WPLOG
C:\Users\Administrator.STIFTUNG>_
```

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

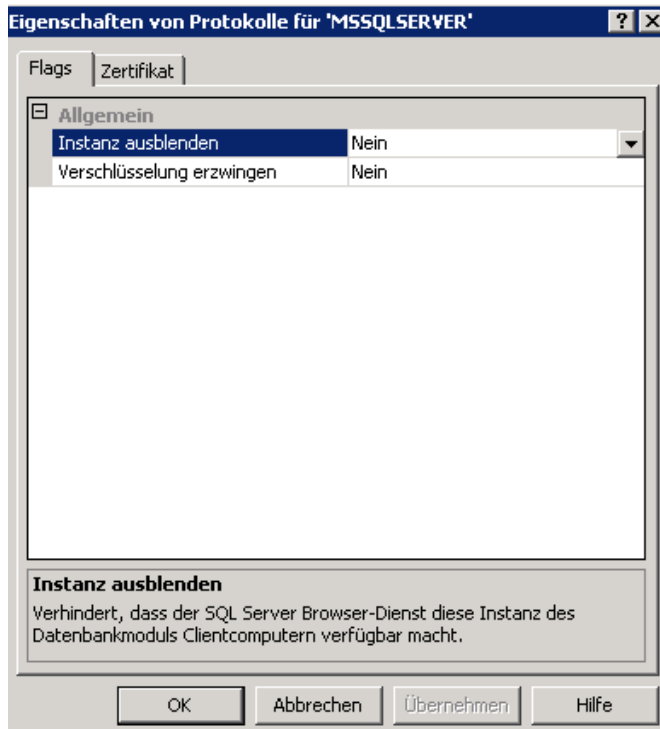


## Benoetigte Rechte

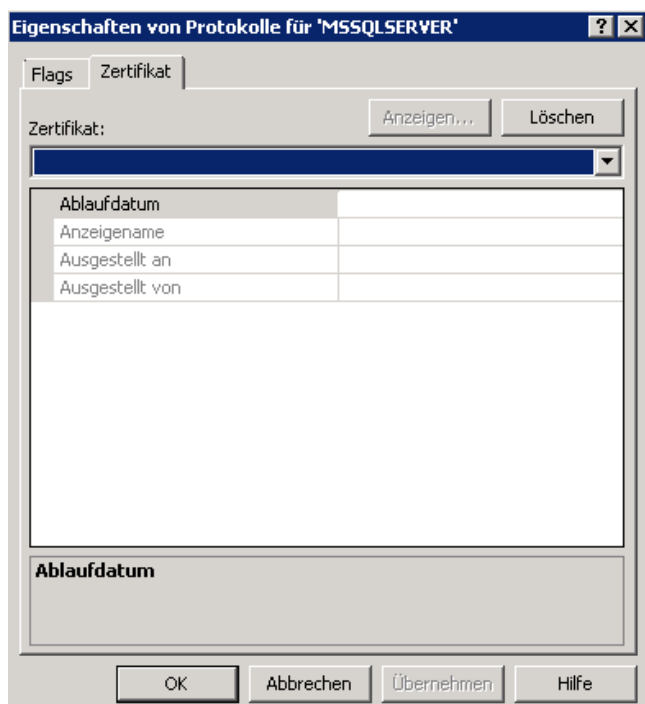


## Verschlüsselung auf dem SQL Server aktivieren

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



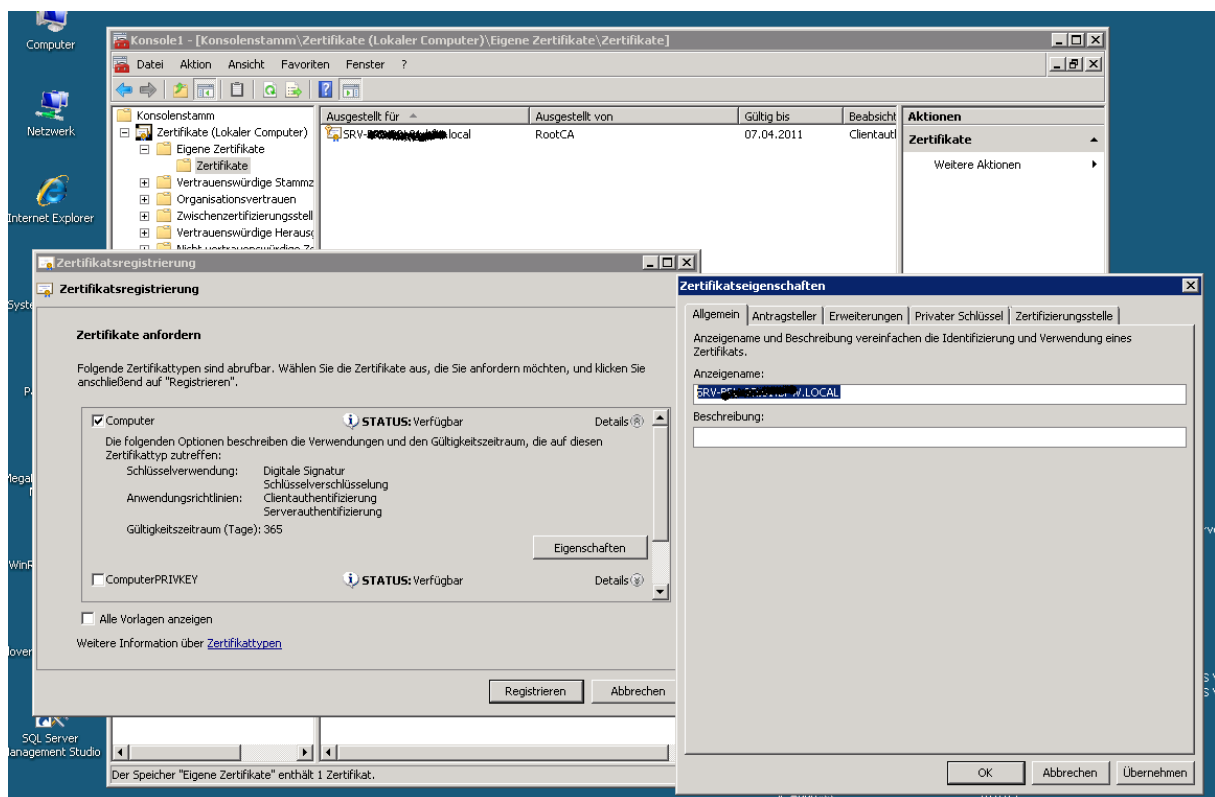
## Kein Zertifikat vorhanden



## Verschlüsselung 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 Eigenschaftensfeld **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

The screenshot shows the 'Zertifikatseigenschaften' dialog box with the 'Erweiterungen' tab selected. The 'Name des Antragstellers' section has a dropdown menu set to 'Allgemeiner Name' and a text box containing 'CN=SRV-E...LOCAL'. The 'Alternativer Name' section has a dropdown menu set to 'Verzeichnisname' and an empty text box. Buttons for 'Hinzufügen >' and '< Entfernen' are visible next to the text boxes. At the bottom, there are 'OK', 'Abbrechen', and 'Übernehmen' buttons.

**Zertifikatseigenschaften**

Allgemein | Antragsteller | **Erweiterungen** | Privater Schlüssel | Zertifizierungsstelle

Der Antragsteller eines Zertifikats ist der Benutzer oder Computer, für den das Zertifikat ausgestellt ist. Geben Sie Informationen über die Arten des Antragstellernamens und alternative Namenswerte ein, die in einem Zertifikat Verwendung finden, ein.

Zertifikatsantragsteller  
Der das Zertifikat empfangende Benutzer oder Computer

Name des Antragstellers:

Typ: [Allgemeiner Name]    Hinzufügen >    CN=SRV-E...LOCAL  
Wert: [ ]    < Entfernen

Alternativer Name:

Typ: [Verzeichnisname]    Hinzufügen >  
Wert: [ ]    < Entfernen

Weitere Informationen über [Subjektnamen](#)

OK    Abbrechen    Übernehmen

## Jetzt kann auch das Zertifikat ausgewählt werden

The screenshot shows the 'Eigenschaften von Protokolle für 'MSSQLSERVER'' dialog box with the 'Zertifikat' tab selected. A dropdown menu shows 'SRV-E...LOCAL'. Below it is a table with certificate details. At the bottom, there are 'OK', 'Abbrechen', 'Übernehmen', and 'Hilfe' buttons.

**Eigenschaften von Protokolle für 'MSSQLSERVER'**

Flags | **Zertifikat**

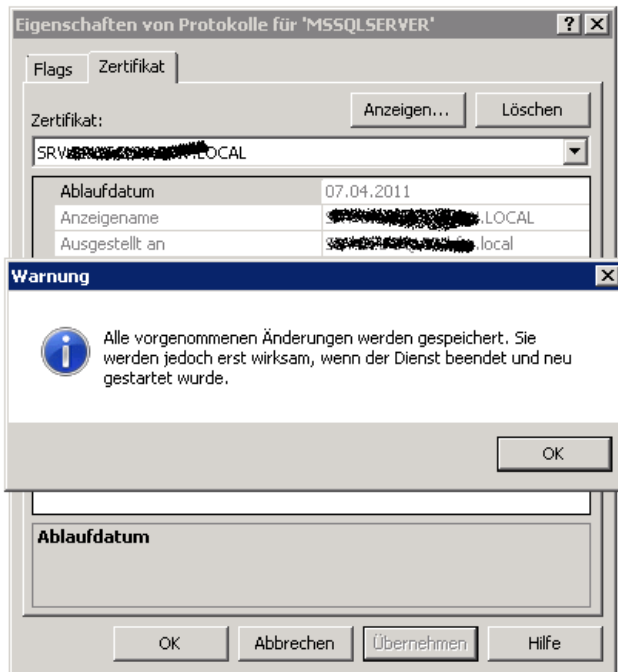
Zertifikat: [SRV-E...LOCAL]    Anzeigen...    Löschen

Ablaufdatum	07.04.2011
Anzeigename	SRV-E...LOCAL
Ausgestellt an	SRV-E...local
Ausgestellt von	local, ...RootCA

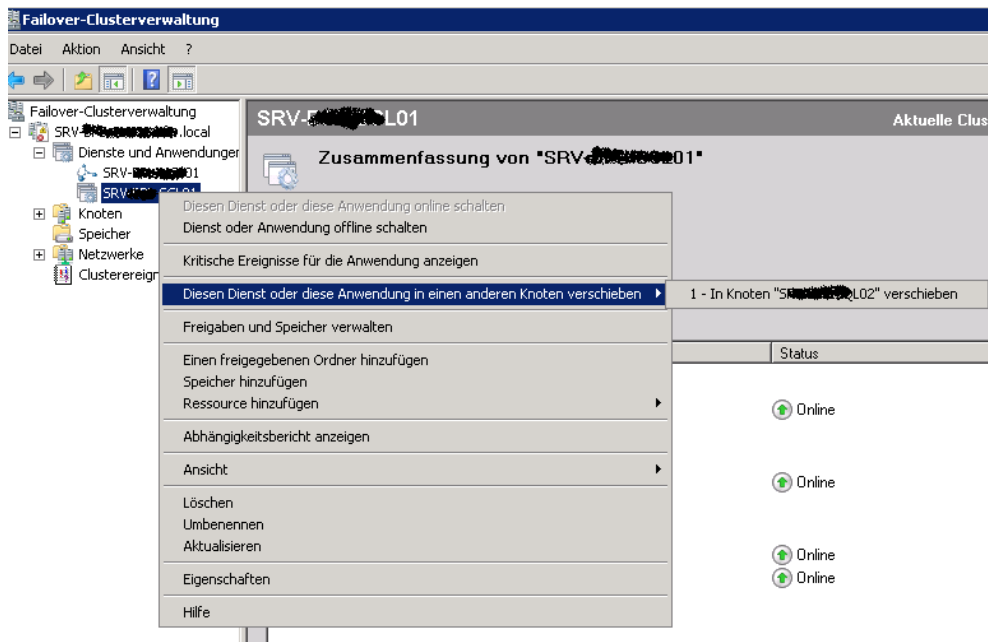
**Ablaufdatum**

OK    Abbrechen    Übernehmen    Hilfe

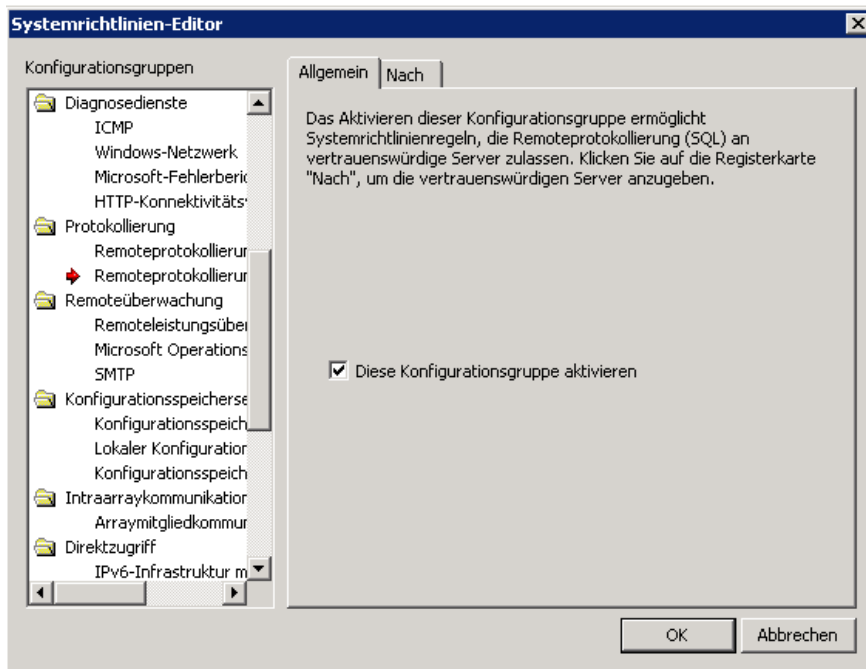
Auch auf dem zweiten SQL Node aktivieren



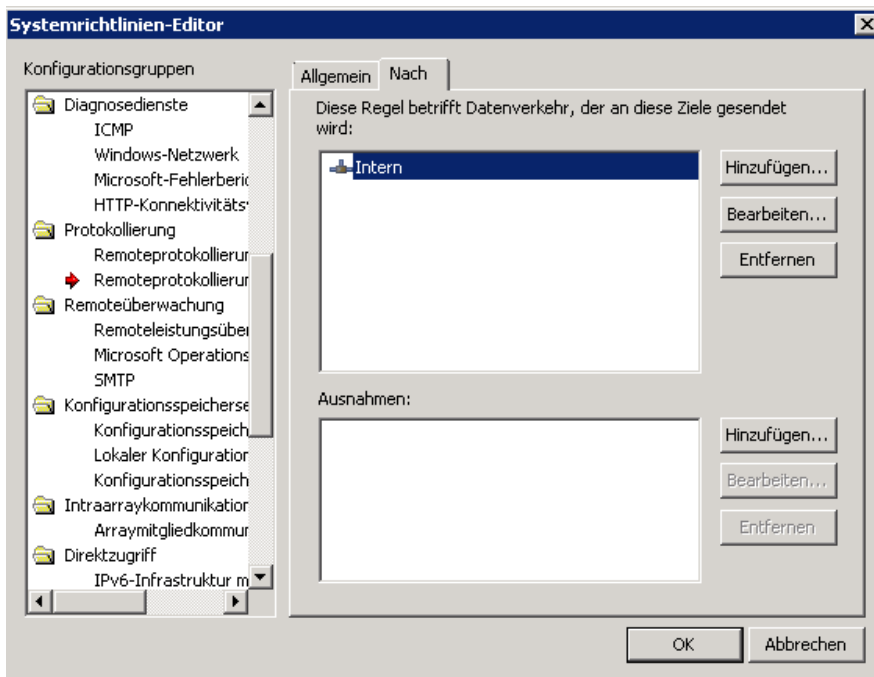
Also einmal einen SQL Cluster Schwenk durchfuehren und die SQL Dienste neu starten



TMG System Policy konfigurieren, das Remote SQL Logging erlaubt ist

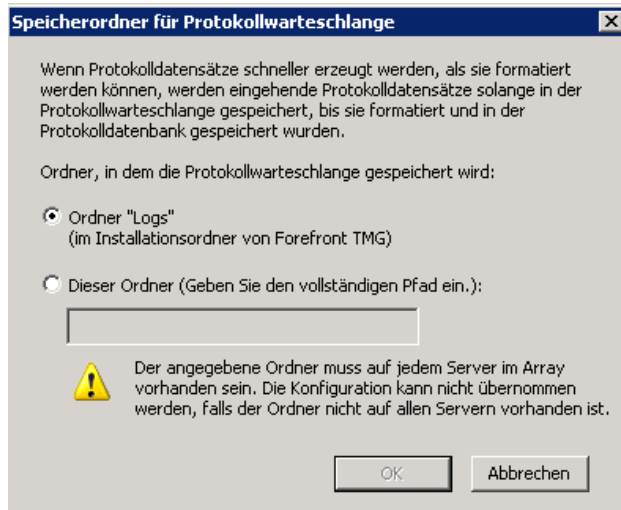


INTERN anpassen auf die SQL Nodes und Cluster Virtual Name / IP



## 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

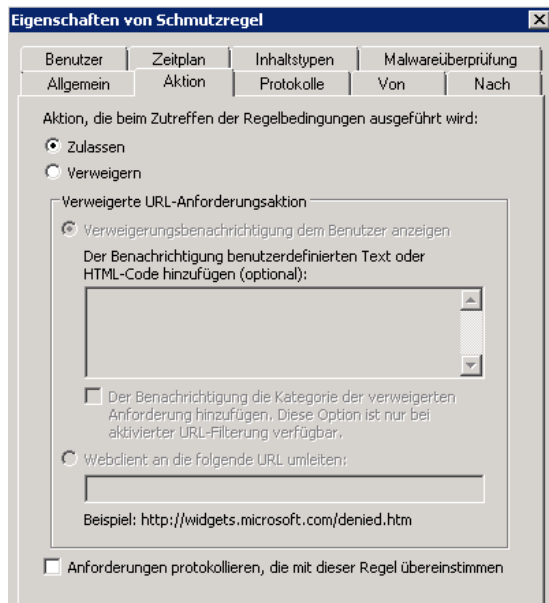
Weitere Informationen zum TMG Firewall Lockdown Modus

<http://www.isaserver.org/tutorials/Explaining-Microsoft-Forefront-TMG-Firewall-Lockdown-Mode.html>

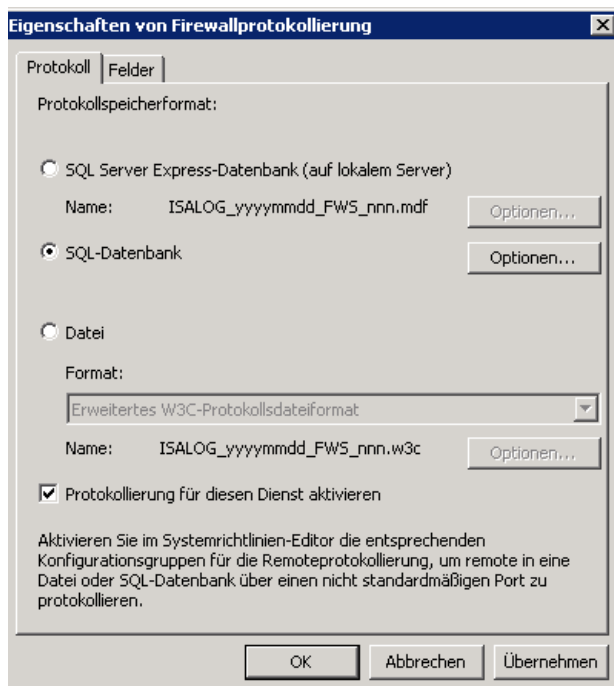
Da TMG sehr viel loggt, kann es Sinn machen, sogenannte Schmutzregeln zu konfigurieren, fuer die nicht notwendiger Traffic (DHCP/NETBIOS etc.) nicht gelogged wird. Damit schont man die Terrabytes auf dem SQL im SAN ☺

Reihenfolge	Name	Aktion	Protokolle	Von / Listener	Nach
1	Schmutzregel	Zulassen	DHCP (Anford... DHCP (Antwort... NetBios-Data... NetBios-Name... NetBios-Sitzung... SNMP SNMP-Trap	Abstrahiert... Intern Lokaler Host Testumgebung Verbindungs... WE WLAN	Lokaler Hos

## Nicht protokollieren



## SQL Logging einschalten



## Angabe des virtuellen SQL Server Cluster Objekts

**Optionen**

Datenbankverbindungsparameter

Server:

Port:

Datenbank:

Tabelle:

Datenverschlüsselung erzwingen

Authentifizierungsdetails

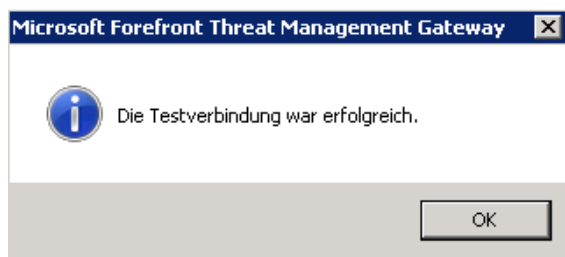
Windows-Authentifizierung verwenden

SQL Server-Authentifizierung verwenden

Benutzer:

Kennwort:

## Testen



# TMGBPA – es ist alles nicht so schlimm wie es aussieht 😊

## View Best Practices Report

TMG-First-Check

Select Report Type:  List Reports  Tree Reports  Other Reports

Has this tool been helpful?  Yes  No

Critical Issues | All Issues | Informational Items

All Issues (24 items)

Print report Export report Find Arrange by: Class

- ✘ The Limit der vor einer IP-Adresse stammenden verweigerten Verbindungen pro Minute überschritten error alert was signaled...
- ✘ The Limit für die globale Rate der abgelehnten Pakete error alert was signaled 1 times
- ✘ Web publishing errors were detected
- ⚠ A policy rule blocks FTP uploads  
The policy rule Clients: TFTP von WE fuer NI blocks FTP uploads. This warning message can be safely ignored if this is your intention. To allow FTP uploads, expand the Firewall Policy node, right-click the policy rule Clients: TFTP von WE fuer NI, click on Configure FTP, and clear the Read Only check box.  
[Do not show me this item again for all instances.](#)
- ⚠ A policy rule blocks FTP uploads
- ⚠ A policy rule blocks FTP uploads
- ⚠ A policy rule blocks FTP uploads
- ⚠ A policy rule blocks FTP uploads
- ⚠ A policy rule blocks FTP uploads
- ⚠ An Exchange Web publishing rule was not created by the proper wizard
- ⚠ An Exchange Web publishing rule was not created by the proper wizard
- ⚠ Forefront TMG Records Logs to the System Drive
- ⚠ One or more certificates in the local computer store do not have a private key
- ⚠ TCP-Acceleration (TCPA) is enabled by the operating system.
- ⚠ The IP-Spoofing warning alert was signaled 1 times
- ⚠ The Komprimierung durch nicht unterstützte Methode warning alert was signaled 1 times
- ⚠ The Konfigurationsfehler warning alert was signaled 10 times
- ⚠ The Service Principal Names (SPNs) for the configuration storage server are not registered in Active Directory
- ⚠ The SYN-Angriff warning alert was signaled 2 times
- ⚠ DNS search order is blank
- ⚠ The current processor speed is less than the maximum possible speed

## 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