

Active Directory-Replikation über Firewalls

(Engl. Originaltitel: [Active Directory Replication over Firewalls](#))

Von Steve Riley

Consultant, Microsoft Telecommunications Practice

März 2001

Firewalls stellen beim Bereitstellen einer verteilten Active Directory™-Verzeichnisdienstarchitektur Schwierigkeiten bei folgenden Aktivitäten dar:

- Erstes Heraufstufen eines Servers zu einem Domänencontroller
- Replizieren des Datenverkehrs zwischen Domänencontrollern

Active Directory verwendet für die Replikation zwischen Domänencontrollern Remoteprozessaufrufe (Remote Procedure Calls, RPCs). (In bestimmten Szenarien kann SMTP [Simple Mail Transfer Protocol] verwendet werden. So z. B. bei der Schema-, Konfigurations- und globalen Katalogreplikation, jedoch nicht der des Domänennamenskontexts, wodurch der Nutzen des Protokolls eingeschränkt ist.) Die ordnungsgemäße Ausführung der Replikation in Umgebungen, in denen eine Verzeichnisgesamtstruktur auf interne DMZ- (demilitarisierte Zonen) und externe Netzwerke (mit Schnittstelle zum Internet) verteilt ist, stellt eine schwierige Aufgabe dar. Es gibt drei mögliche Ansätze:

- Ein weites Öffnen des Firewalls, um das systemeigene dynamische Verhalten von RPCs zuzulassen.
- Das Beschränken der RPC-Verwendung durch TCP-Ports bei nur geringfügigem Öffnen des Firewalls.
- Das Kapseln des Domänencontrollerverkehrs (zwischen Domänencontrollern) im IPSec-Protokoll (IP Security Protocol), für das der Firewall geöffnet werden soll.

Jeder Ansatz hat Vor- und Nachteile. Im Allgemeinen stehen oben auf der Liste mehr Nach- als Vorteile. Unten auf der Liste ist es umgekehrt. Obgleich dieses Dokument alle drei Ansätze beschreibt, liegt der Schwerpunkt auf der IPSec-Methode, da diese Vorteile gegenüber den anderen beiden bietet.

Voll dynamische RPCs

Vorteile	Nachteile
Keine spezielle Serverkonfiguration	Durchlöchert den Firewall
	Willkürlich eingehende Verbindungen über Ports mit hohen Nummern
	Unsichere Firewallkonfiguration

Obwohl die Konfiguration einer Umgebung auf diese Weise möglich ist, gibt es zahlreiche Gründe, darauf zu verzichten, da ein unsicheres Netzwerk die Folge ist. Dieser Ansatz erfordert jedoch den geringsten Konfigurationsaufwand.

Um die Replikation über dynamische RPCs zu ermöglichen, muss der Firewall so konfiguriert werden, dass Folgendes zugelassen wird.

Dienst	Port/Protokoll
RPC-Endpunktzuordnung	135/TCP, 135/UDP
NetBIOS-Namensdienst (Network Basic Input/Output System)	137/TCP, 137/UDP
NetBIOS-Datagrammdienst	138/UDP
NetBIOS-Sitzungsdienst	139/TCP
Dynamische RPC-Zuweisung	1024-65535/TCP
SBM (Server Message Block) über IP (Microsoft-DS)	445/TCP, 445/UDP
LDAP (Lightweight Directory Access Protocol)	389/TCP
LDAP über SSL	636/TCP
LDAP für globalen Katalog	3268/TCP
LDAP für globalen Katalog über SSL	3269/TCP
Kerberos	88/TCP, 88/UDP
Domain Name Service (DNS)	53/TCP ¹ , 53/UDP
WINS-Auflösung (Windows Internet Naming Service), falls erforderlich	1512/TCP, 1512/UDP
WINS-Replikation (falls erforderlich)	42/TCP, 42/UDP

Es ist die eigentliche "dynamische RPC-Zuweisung", die dieses Szenario unsicher macht. Diese Zuweisung, die sich auf hohe TCP-Ports bezieht, muss eingehenden Datenverkehr an allen Ports über 1023 zulassen. Wenn Ihr Firewall dies zulässt, gibt es eigentlich keinen Grund, überhaupt einen Firewall einzusetzen.

Wenn Sie DNS oder WINS nicht zulassen möchten, können Sie **HOSTS**- (für DNS) und **LMHOSTS**-Dateien (für WINS) für die Namensauflösung verwenden. Der Speicherort dieser Dateien ist **%Systemstamm%\System32\Drivers\Etc**. Informationen zur Verwendung der Dateien enthalten die Dateien selbst.

Funktionsweise von RPC

Ein RPC-Dienst konfiguriert sich in der Registrierung mithilfe einer universellen eindeutige Bezeichnung (Universally Unique Identifier, UUID), die einer globalen eindeutigen Bezeichnung (Globally Unique Identifier, GUID) ähnelt. UUIDs sind bekannte Bezeichnungen, die für jeden Dienst eindeutig und auf allen Plattformen gängig sind. Beim Start eines RPC-Diensts erhält dieser einen freien hohen Port, der mit der UUID registriert wird. Einige Dienste verwenden wahlfreie hohe Ports. Andere versuchen, dieselben hohen Ports ständig zu verwenden, falls diese verfügbar sind. Für die Lebensdauer des Dienstes ist die Portzuweisung statisch.

Wenn ein Client mit einem bestimmten RPC-Dienst kommunizieren möchte, ist es ihm nicht möglich, den Port im Voraus zu bestimmen, an dem der Dienst ausgeführt wird. Der Client baut eine Verbindung zum Portzuweisungsdienst des Servers (an 135) auf und fordert den gewünschten Dienst mithilfe der UUID des Dienstes an. Der Portzuweisungsdienst gibt die entsprechende Portnummer an den Client zurück und schließt die Verbindung. Schließlich erstellt der Client eine neue Verbindung zu dem Server mithilfe der Portnummer, die vom Portzuweisungsdienst empfangen wurde.

Da es unmöglich ist, im Voraus zu wissen, welchen Port ein RPC-Dienst verwenden wird, muss der Firewall Datenverkehr durch alle hohen Ports zulassen.

Begrenzte RPCs

Vorteile	Nachteile
Sicherer als dynamische RPCs, da nur ein hoher Port geöffnet ist	Registrierungsänderung auf allen Servern

Dieses Szenario bietet mehr Sicherheit, erfordert jedoch Registrierungsänderungen auf allen Domänencontrollern. Registrierungsänderungen können mithilfe von Tools in *Microsoft Windows 2000 – Die technische Referenz* skriptgesteuert ausgeführt werden, wodurch Konfigurationsfehler vermieden werden.

Für die RPC-Replikation müssen Sie eine feste Portnummer festlegen. Die IANA (Internet Assigned Numbers Authority) hat für private und dynamische Zuweisungen den Bereich 49152 bis 65535 vorgegeben.

Wechseln Sie im Registrierungs-Editor zu folgendem Registrierungsschlüssel:

HKEY_LOCAL_MACHINE
SYSTEM
CurrentControlSet
Services
NTDS
Parameters

Fügen Sie den neuen DWORD-Wert **TCP/IP Port** (einschließlich Leerzeichen) hinzu. Legen Sie den Wert auf die gewünschte Portnummer fest. Vergessen Sie nicht, die angezeigte Basis auf dezimal festzulegen, ehe Sie die Daten eingeben. Geben Sie auf allen Servern so vor, auf denen Active Directory ausgeführt wird. Sie müssen die Server neu starten, damit die Änderung wirksam wird.

Konfigurieren Sie nun Ihre Firewall so, dass Folgendes zugelassen wird:

Dienst	Port/Protokoll
RPC-Endpunktzuordnung	135/TCP, 135/UDP
NetBIOS-Namensdienst	137/TCP, 137/UDP
NetBIOS-Datagrammdienst	138/UDP
NetBIOS-Sitzungsdienst	139/TCP
Statischer RPC-Port für Active Directory-Replikation	<Fester Port>/TCP
SMB über IP (Microsoft-DS)	445/TCP, 445/UDP
LDAP	389/TCP
LDAP über SSL	636/TCP
LDAP für globalen Katalog	3268/TCP
LDAP für globalen Katalog über SSL	3269/TCP
Kerberos	88/TCP, 88/UDP
DNS	53/TCP, 53/UDP
WINS-Auflösung (falls erforderlich)	1512/TCP, 1512/UDP
WINS-Replikation (falls erforderlich)	42/TCP, 42/UDP

Ersetzen Sie <Fester Port> durch die Portnummer, die Sie in den Registrierungswert eingegeben haben.

Wenn Sie wie zuvor DNS oder WINS nicht zulassen möchten, können Sie **HOSTS-** (für DNS) und **LMHOSTS-** Dateien (für WINS) für die Namensauflösung verwenden. Der Speicherort dieser Dateien ist **%Systemstamm%\System32\Drivers\Etc**. Informationen zur Verwendung der Dateien enthalten die Dateien selbst.

Sie benötigen weiterhin die Endportzuweisung, da den Clients nicht bekannt ist, dass Sie den Port fest eingestellt haben. Die Endportzuweisung gibt stets den festen Port zurück, wenn Clients die Portnummer anfordern, die der RPC-UUID von Active Directory zugeordnet wurde.

Es folgt nun Text, den Sie in die Registrierung importieren können. Dabei wird der Port auf **49152** festgelegt. Kopieren Sie den Text in die Zwischenablage, fügen Sie ihn in ein leeres Editor-Dokument ein, speichern Sie die Datei mit der Erweiterung REG, und doppelklicken Sie in Windows-Explorer auf diese Datei. Wenn Sie einen anderen Port verwenden möchten, öffnen Sie den Windows-Rechner (im wissenschaftlichen Modus), um die Zahl von dezimal nach hexadezimal zu konvertieren. Setzen Sie vor den Wert vier führende Nullen, wie in folgendem Beispiel gezeigt.

Windows-Registrierungs-Editor, Version 5.00

```
[HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \NTDS \Parameters]
"TCP/IP Port"=dword:0000c000
```

Kapseln in IPSec

Vorteile	Nachteile
Bietet die beste Firewallsicherheit	IPSec-Richtlinienkonfiguration auf allen Servern
Gegenseitig Authentifizierung zwischen Domänencontrollern	
Einzel festgelegte Richtlinien, falls erforderlich	
Guter Grund, um auf Wunsch mit dem Bereitstellen einer öffentlichen Schlüsselinfrastruktur zu beginnen	

IPSec bietet eine Möglichkeit, RPC-Datenverkehr zu kapseln und mühelos über einen Firewall zu übertragen. Neben dem Vereinfachen des RPC-Transports erhöht IPSec auch aufgrund des gegenseitigen Authentifizierungsfeatures zwischen Domänencontrollern die Sicherheit. Durch das Verwenden von entweder Kerberos oder Computerzertifikaten ist den Domänencontrollern bekannt, mit wem sie kommunizieren, ehe ein tatsächlicher Informationsaustausch erfolgt.

Dieses Dokument erläutert das Erstellen einer geeigneten IPSec-Richtlinie unter Verwendung der MMC-Benutzeroberfläche (Microsoft Management Console). Sie können die Richtlinienerstellung mit dem Tool **IPSECPOL.EXE**, das in *Windows 2000 – Die technischer Referenz* enthalten ist, skriptgesteuert ausführen. Lesen Sie sorgfältig die Dokumentation zu **IPSECPOL.EXE**, damit Sie mit dem Tool vor seiner Verwendung vertraut sind. Im Gegensatz zur grafischen Benutzeroberfläche ist in das Befehlszeilenprogramm die Konsistenzprüfung nur geringfügig integriert.

Bevor Sie beginnen, müssen Sie festlegen, ob Sie Zertifikate für die IPSec-Authentifizierung oder die integrierte Kerberos²-Authentifizierung für Windows 2000 verwenden möchten. Die Kerberos-Authentifizierung erfordert, dass beide Computer sich bereits in derselben Domäne befinden. Wenn Sie also Kerberos bevorzugen, müssen in der Domänencontroller-Heraufstufungsphase (DCPROMO) ein anderes Protokoll als IPSec verwenden, da der Zielservers noch kein Mitglied der Domäne ist. PPTP-Tunnel (Point-to-Point Tunneling Protocol) sind für diesen Zweck gut geeignet und werden im Folgenden beschrieben. Wenn Sie für die Authentifizierung Zertifikate verwenden möchten, müssen Sie für jeden Domänencontroller, der an der IPSec-Replikation beteiligt ist, ein Zertifikat abrufen. Unter <http://www.microsoft.com/windows2000/techinfo/default.asp> (englischsprachig) finden Sie Dokumente, die das Erstellen einer Windows 2000-Zertifizierungsstelle und das Konfigurieren einer Domäne für die automatische Registrierung von Computerzertifikaten erläutern.

Um die IPSec-Replikation und die IPSec- oder PPTP-Heraufstufung zu ermöglichen, muss der Firewall so konfiguriert werden, dass Folgendes zugelassen wird.

Dienst	Port/Protokoll
DNS	53/TCP, 53/UDP
PPTP-Einrichtung (beim Verwenden von PPTP)	1723/TCP
GRE (Generic Routing Encapsulation) (beim Verwenden von PPTP)	IP-Protokoll 47
Kerberos ³	88/TCP, 88/UDP
IKE (Internet Key Exchange)	500/UDP
IPSec-ESP (Encapsulated Security Payload)	IP-Protokoll 50
IPSec-AH (Authenticated Header)	IP-Protokoll 51

Beachten Sie, dass IPSec über NAT-Geräte (Network Address Translation) nicht ausgeführt werden kann. Da IPSec zum Berechnen von Paketprüfsummen IP-Adressen verwendet, werden IPSec-Pakete, deren Quelladressen von NAT geändert würden, beim Erreichen des Ziels zurückgewiesen.

Heraufstufung von Domänencontrollern mithilfe von PPTP-Tunneln

Wenn Sie für die Heraufstufungsphase PPTP-Tunnel wählen, müssen Sie im internen Netzwerk den Routing- und RAS-Dienst (RRAS) konfigurieren. Der RRAS-Dienst kann entweder auf einem internen Domänencontroller oder einem getrennten Server ausgeführt werden. Zur Vereinfachung sollte sich der RRAS-Server am besten in demselben Subnetz wie der Stammdomänencontroller befinden, weil dadurch kein statischer Leitweg erhalten bleiben muss.

So konfigurieren Sie den RRAS-Dienst

- Klicken Sie auf **Start**, zeigen Sie auf **Programme**, dann auf **Verwaltung**, und klicken Sie auf **Routing und RAS**.
- Klicken Sie im linken Bereich mit der rechten Maustaste auf den gewünschten Server, und klicken Sie dann auf **Routing und RAS konfigurieren und aktivieren**. Der Setup-Assistent für den Routing- und RAS-Server wird gestartet.
- Klicken Sie auf **Manuell konfigurierter Server (Manually configured server)**.

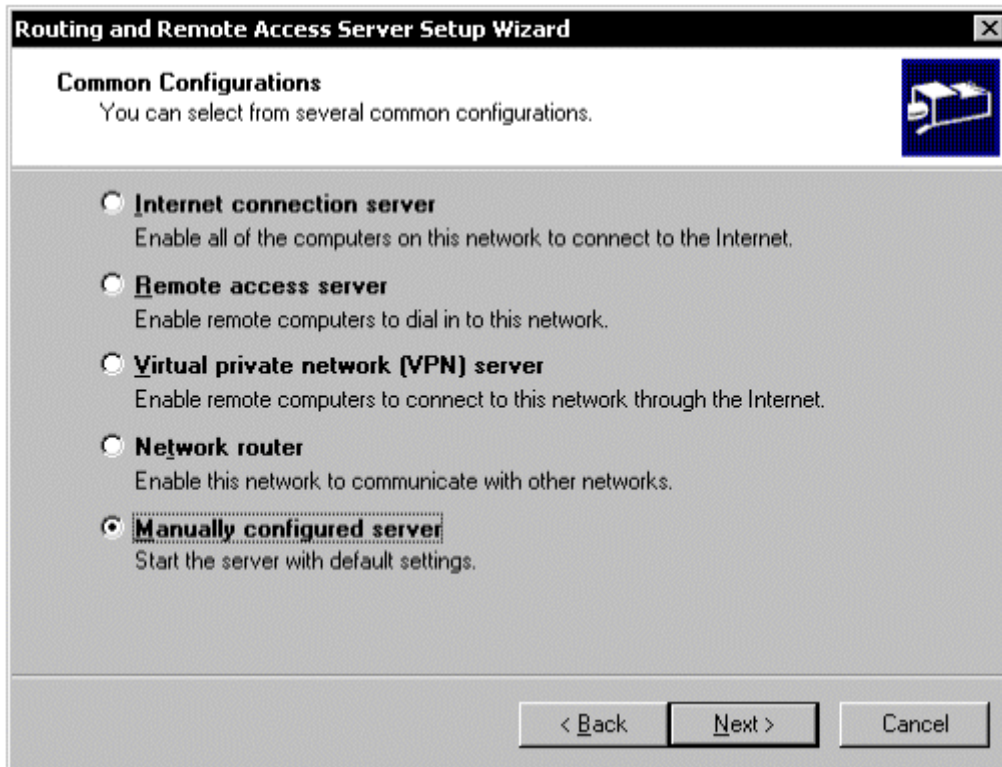


Abbildung 1: Setup-Assistent für den Routing- und RAS-Server

- Schließen Sie den Assistenten ab, und starten Sie nach Aufforderung den Dienst.

Nachdem Sie auf das Plus-Zeichen neben dem Servernamen geklickt haben, sollte MMC folgendermaßen aussehen.

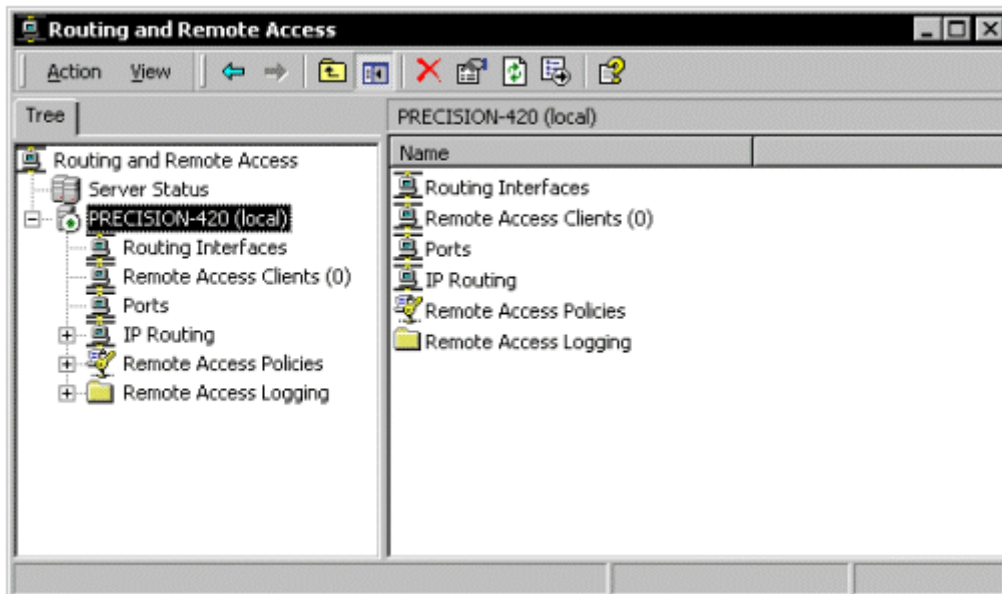


Abbildung 2: Der RRAS-Dienst nach Konfiguration und Aktivierung

Nehmen Sie nach der Konfiguration und Aktivierung des RRAS-Dienstes die folgenden Änderungen vor:

- Klicken Sie mit der rechten Maustaste auf den Server, und klicken Sie dann auf **Eigenschaften (Properties)**. Klicken Sie auf die Registerkarte **IP**. Klicken Sie auf **Statischen Adresspool (Static address pool)**. Geben Sie in das Subnetz des internen Domänencontrollers einen IP-Adressbereich ein. Es sind nur wenige Adressen (höchstens 9) erforderlich. Schließen Sie alle Dialogfelder.

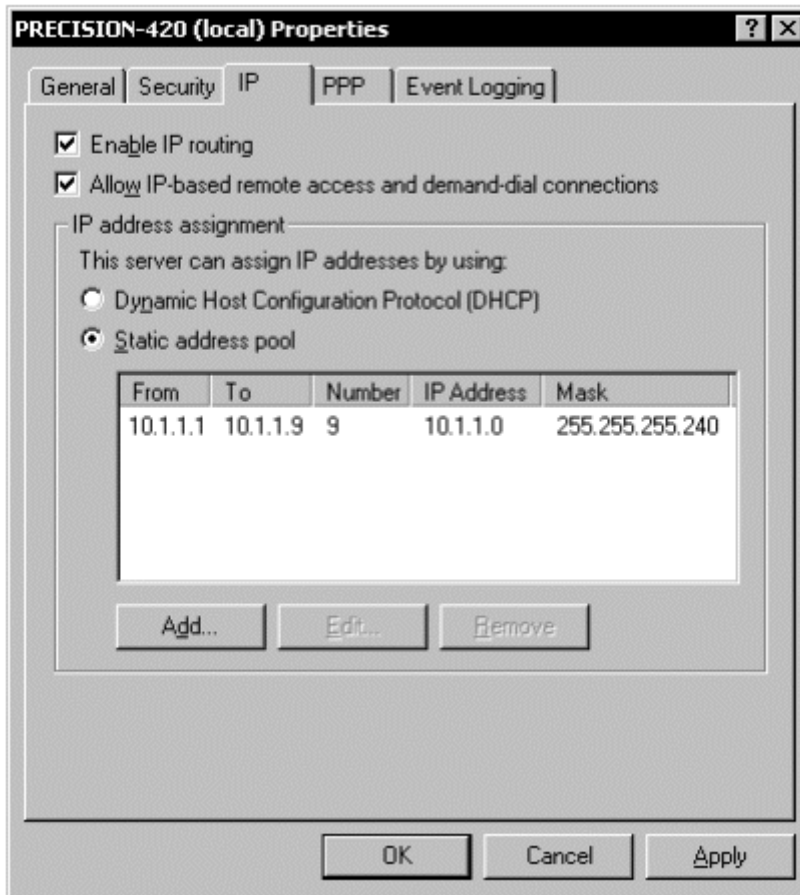


Abbildung 3: Servereigenschaften und IP-Adresszuweisung

- Klicken Sie mit der rechten Maustaste im linken Bereich von MMC auf **Ports**, und klicken Sie dann auf **Eigenschaften (Ports Properties)**. Konfigurieren Sie **Parallelanschluss (direkt) (Direct parallel)** so, dass weder RAS- noch bei Bedarf herzustellende Verbindungen zugelassen werden. Wenn an den Server Modems angeschlossen sind (wie im Beispiel unten), konfigurieren Sie diese ebenso. Konfigurieren Sie **Wählen bei Bedarf (L2TP)** so, dass keine Nullports vorhanden sind und weder RAS- noch bei Bedarf herzustellende Verbindungen zugelassen werden. An **Wählen bei Bedarf (PPTP)** müssen keine Änderungen vorgenommen werden, es sei denn, Sie benötigen mehr als fünf Ports. Schließen Sie alle Dialogfelder.

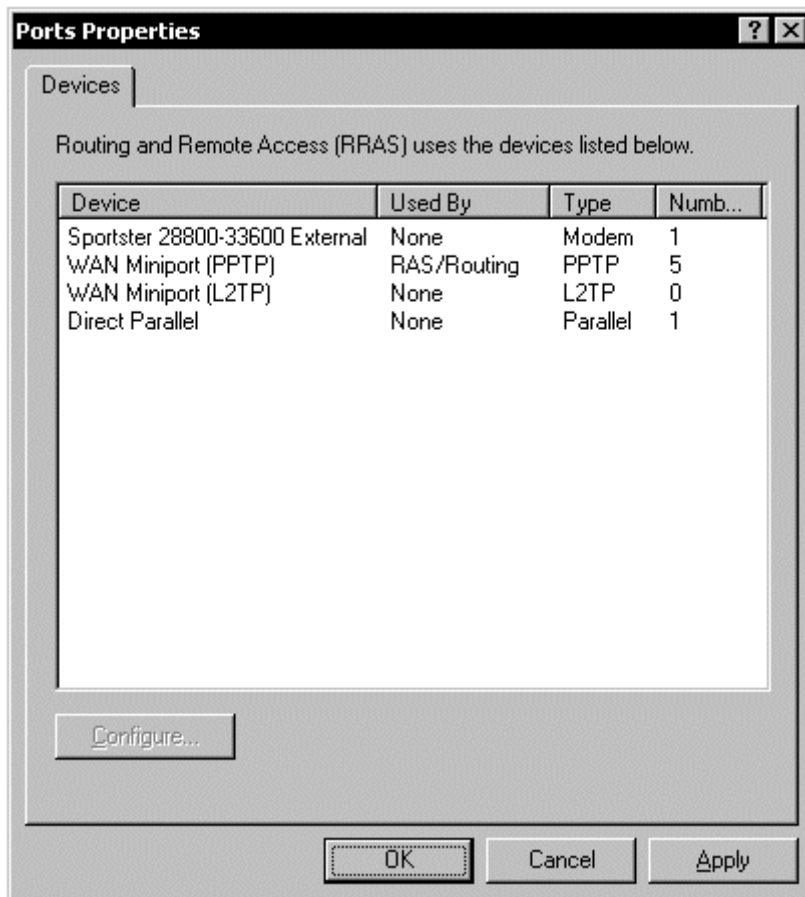


Abbildung 4: Eigenschaften der Ports

Der RRAS-Dienst kann nun eingehende PPTP-Verbindungen für die Heraufstufung von Domänencontrollern akzeptieren.

Richten Sie vor dem Heraufstufen einer DMZ oder eines externen Servers zu einem Domänencontroller einen PPTP-Tunnel zum internen RRAS-Server ein. Öffnen Sie die Seite **Eigenschaften** von **Netzwerkumgebung**, und klicken Sie auf **Neue Verbindung erstellen**. Führen Sie im Assistenten folgenden Schritte aus:

- Klicken Sie auf **Verbindung mit einem privaten Netzwerk über das Internet herstellen**.
- Wählen Sie keine Eingangsverbindung.
- Geben Sie die IP-Adresse des internen RRAS-Servers als Ziel ein.
- Legen Sie die Verfügbarkeit der Verbindung auf **Für alle Benutzer verwenden** fest.
- Geben Sie die Verbindung nicht für die gemeinsame Nutzung frei.
- Benennen Sie die Verbindung nach Wunsch.

Die Verbindung wird geöffnet. Klicken Sie vor dem Aufbau der Verbindung auf die Schaltfläche **Eigenschaften**. Klicken Sie auf die Registerkarte **Optionen** und dann auf **Windows-Anmelde-domäne einbeziehen**. Schließen Sie das Dialogfeld.

Melden Sie sich nun beim RRAS-Server mit den Anmeldeinformationen des Organisationsadministrators (des Administrators der Stammdomäne) an. Nachdem der Server die Verbindung aufgebaut hat, können Sie DCPRMO starten. DCPRMO erfordert am Ende des Vorgangs einen Neustart, bei dem auch der PPTP-Tunnel abgetrennt wird. Da Sie den Tunnel nicht mehr benötigen, können Sie die Verbindung löschen.

Heraufstufung von Domänencontrollern mithilfe von IPSec und Computerzertifikaten

Sie können diese Methode wählen, wenn eine der folgenden Voraussetzungen gilt:

- Sie möchten PPTP nicht für die Heraufstufung verwenden.
- Sie möchten Kerberos nicht die Durchleitung durch den Firewall gestatten.
- Sie suchen nach einem Grund, um mit dem Bereitstellen einer öffentlichen Schlüsselinfrastruktur zu beginnen.

Sie müssen alle Zertifikate auf den Domänencontrollern installieren, damit diese die IPSec-Authentifizierung durchführen können. Alle Zertifikate benötigen Signaturen derselben Zertifizierungsstelle. Windows 2000 enthält eine Request for Comments-Zertifizierungsstelle (RFC-kompatibel), die in diesem Fall sehr gut geeignet ist. Mittels Gruppenrichtlinien können Sie Ihre Domäne so konfigurieren, dass Mitgliedscomputer automatisch mit Computerzertifikaten registriert werden. Während IPSec Zertifikate einer beliebigen Zertifizierungsstelle akzeptiert, ist für die automatische Registrierung eine Windows 2000-Zertifizierungsstelle erforderlich. Wenn Sie bereits über eine öffentliche Schlüsselinfrastruktur verfügen, kann die Windows 2000-Zertifizierungsstelle als untergeordnete Zertifizierungsstelle konfiguriert werden, indem Sie eine Zertifizierungsstelle ausgeben. Weitere Informationen sowie die zuvor erwähnten Leitfäden finden Sie in der Dokumentation.

Bei Wahl dieser Methode können Sie den Kerberos-Datenverkehr in IPSec einbeziehen. Normalerweise werden bestimmte Datenverkehrsarten von der IPSec-Transportmodusverarbeitung nicht berücksichtigt:

- **Broadcasts.** Können nicht von den IPSec-Filtern klassifiziert werden, da der Absender nicht alle Empfänger kennt.
- **Multicast.** (Siehe Broadcast).
- **RSVP (Resource Reservation Protocol), IP-Protokoll 46.** Bleibt unberücksichtigt, damit eine QoS-Markierung (Quality of Service) erfolgt. IPSec-Pakete können jedoch in RSVP-Paketen übertragen werden.
- **IKE (Internet Key Exchange).** Wird von IPSec verwendet, um Sicherheitsparameter einzurichten und Schlüssel auszutauschen. IKE-Aushandlungen sind bereits entsprechend verschlüsselt.
- **Kerberos.** Das systemeigene Windows 2000-Authentifizierungsprotokoll, das auch von IPSec für die Computerauthentifizierung verwendet wird. Kerberos selbst ist bereits sicher.

Auch wenn ein IPSec-Filter angeben sollte, dass der gesamte von einem Computer stammende Datenverkehr gekapselt werden soll, sind die zuvor genannten Datenverkehrsarten von der IPSec-Verarbeitung ausgeschlossen.

Windows 2000 Service Pack 1 enthält einen Registrierungsschlüssel, der dieses Verhalten geringfügig ändert. Wechseln Sie im Registrierungs-Editor zu folgendem Registrierungsschlüssel:

```
HKEY_LOCAL_MACHINE
SYSTEM\
CurrentControlSet\
Services\
IPSEC\
```

Fügen Sie den neuen DWORD-Wert **NoDefaultExempt** hinzu, und legen Sie dessen Wert auf **1** fest. Die folgenden Werte sind möglich:

- 0:** Standardausnahmen gelten
- 1:** Kerberos und RSVP werden in die IPSec-Verarbeitung einbezogen

Das Einbeziehen von Kerberos in IPSec ist kein Problem, wenn ein Computer zuvor zu einem Domänencontroller heraufgestuft wurde (und so Mitglied der Domäne ist). Doch für einen Computer, der noch nicht Mitglied einer Domäne ist und den Sie zu einem Domänencontroller heraufstufen möchten, können Sie Kerberos nicht in IPSec einbeziehen. Sie müssen eine andere Form der Authentifizierung wählen, was der Grund für das Verwenden von Computerzertifikaten ist.

Es folgt nun Text, den Sie in die Registrierung importieren können. Dabei wird der Wert **NoDefaultExempt** auf **1** festgelegt. Kopieren Sie den Text in die Zwischenablage, fügen Sie ihn in ein leeres Editor-Dokument ein, speichern Sie die Datei mit der Erweiterung .REG, und doppelklicken Sie in Windows-Explorer auf diese Datei.

Windows-Registrierungs-Editor, Version 5.00

```
[HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \IPSEC]
"NoDefaultExempt"=dword:00000001
```

Ihnen müssen die Auswirkungen dieses Schrittes bewusst sein. Wenn Sie diese Methode wählen, müssen Sie alle Schritte im nächsten Abschnitt, "Konfigurieren des IPSec-Transportmodus für die Kommunikation zwischen Domänencontrollern", befolgen, *ehe* Sie DCPRMO ausführen. Beachten Sie diese Reihenfolge:

1. Wenn Sie Kerberos in die IPSec-Verarbeitung einbeziehen möchten, fügen Sie den vorherigen Registrierungsschlüssel hinzu.
2. Installieren Sie eine Zertifizierungsstelle.
3. Rufen Sie Computerzertifikate für alle vorhandenen und vorgesehenen Domänencontroller ab.
4. Führen Sie die im Abschnitt "Konfigurieren des IPSec-Transportmodus für die Kommunikation zwischen Domänencontrollern" genannten Schritte durch.
5. Führen Sie DCPRMO auf allen vorgesehenen Domänencontrollern aus.
6. Führen Sie danach keine Änderungen mehr durch. Die Replikation erfolgt nun über die vorhandene IPSec-Konfiguration.

Vergleich der beiden Heraufstufungsmethoden

Es folgen nun die Unterschiede zwischen den beiden zuvor vorgestellten Methoden.

PPTP-Tunnel

- Einfach und schnell.
- Der Firewall muss Kerberos-Datenverkehr zulassen.
- Der Firewall muss PPTP-Datenverkehr zulassen.
- Trennt die Heraufstufungs- von den Replikationsfunktionen. Konfigurieren Sie PPTP für die Heraufstufung und anschließend IPSec für die nachfolgende Replikation.

IPSec mit Computerzertifikaten

- Bietet einen guten Grund für das Bereitstellen einer öffentlichen Schlüsselinfrastruktur.
- Ermöglicht die Einbeziehung von Kerberos in die IPSec-Verarbeitung.
- Lässt weniger Protokolle durch den Firewall zu. Nicht PPTP und möglicherweise auch nicht Kerberos.
- Für Heraufstufung und nachfolgende Replikation ist nur ein Schritt erforderlich.

Obwohl keine Methode Vorteile gegenüber der anderen hat, ist das Verwenden von IPSec mit Computerzertifikaten ein "zukunftsorientierterer" Ansatz, da die meisten Unternehmen die Bereitstellung einer öffentlichen Schlüsselinfrastruktur planen.

Konfigurieren des IPSec-Transportmodus für die Kommunikation zwischen Domänencontrollern

Nun müssen auf allen Domänencontrollern Richtlinien konfiguriert werden, damit für die Kommunikation untereinander der IPSec-Transportmodus verwendet wird. Bei dieser Konfiguration dürfen Sie nur IPSec und verwandten Protokollen die Durchleitung durch den Firewall gestatten, was eine Vereinfachung darstellt und die Unterstützung erleichtert. Dabei werden jedoch keine IPSec-Tunnel erstellt. Stattdessen verwenden Sie den IPSec-Transportmodus von Endpunkt zu Endpunkt, um die Kommunikationssitzungen zwischen den Servern zu schützen.

Sie müssen auf allen Domänencontrollern eine IPSec-Richtlinie für die Replikation sowie eine entsprechende IP-Filterliste und Filteraktion erstellen. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, dann auf **Verwaltung**, und klicken Sie auf **Lokale Sicherheitsrichtlinie (Local Security Policy)**.

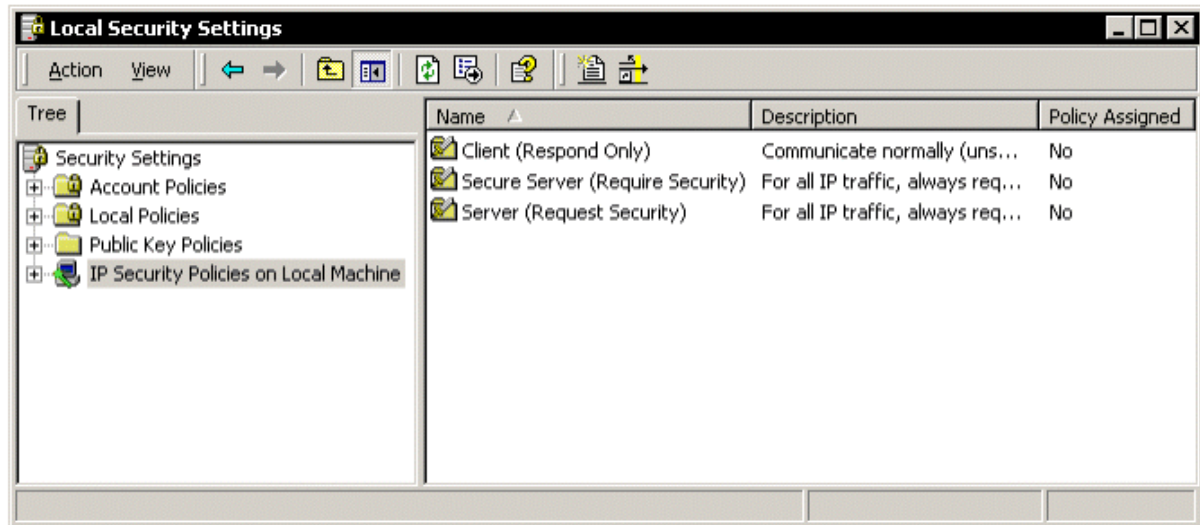


Abbildung 5: Lokale Sicherheitseinstellungen

Klicken Sie anschließend im linken Bereich von MMC auf **IP-Sicherheitsrichtlinien auf lokalem Computer (IP Security Policies on Local Machine)**. Dadurch werden die Standardrichtlinien angezeigt, denen Sie eine neue Richtlinie für die Replikation hinzufügen. Zuvor müssen Sie jedoch die Filterliste und -aktion erstellen.

Die Filterliste gibt an, welche IP-Adressen, Ports und Protokolle die Anwendung von IPSec auslösen. Sie möchten nur den gesamten Datenverkehr zwischen den Domänencontrollern und nicht den Datenverkehr zwischen einem Domänencontroller und einem anderen Computer schützen. Klicken Sie im rechten Bereich von MMC mit der rechten Maustaste auf **IP-Filterlisten und Filteraktion verwalten (Manage IP filter lists and filter actions)**. Sie befinden sich nun auf der Registerkarte **IP-Filterlisten verwalten (Manage IP Filter Lists)**. Eine Filterliste enthält verschiedene Filter. *Sie erstellen einen Filter für jeden Server, der mit diesem Server an der Replikation teilnimmt.* Das bedeutet, dass nur eine Filterliste erforderlich ist und dass die Liste Filter für alle Domänencontroller enthält.

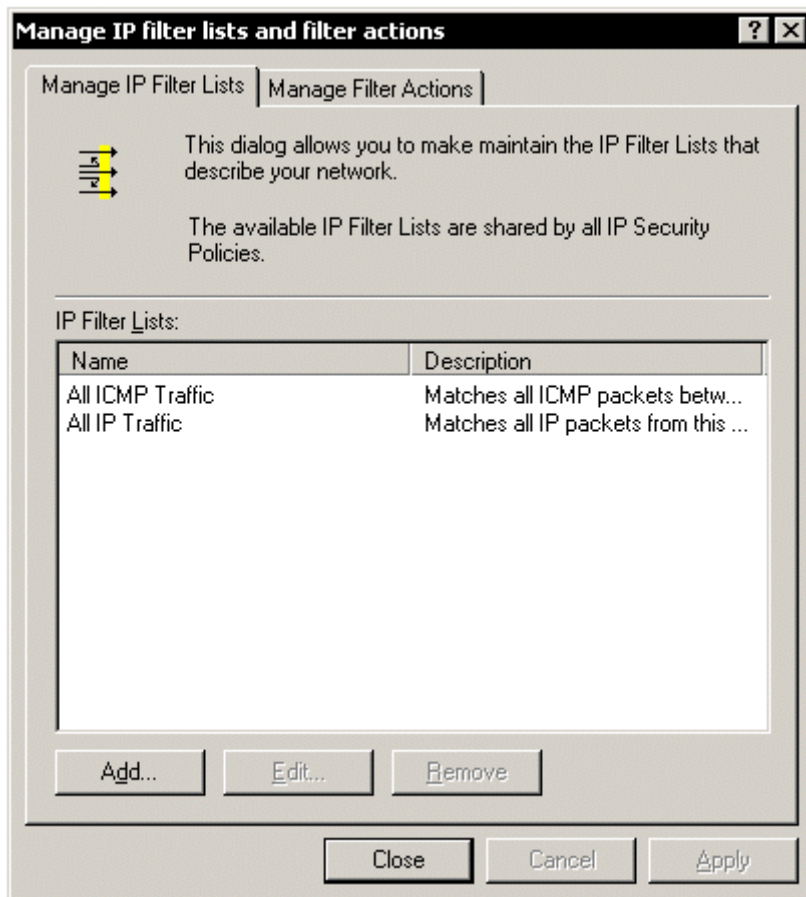


Abbildung 6: IP-Filterlisten und Filteraktionen. Registerkarte mit IP-Filterlisten

Klicken Sie auf die Schaltfläche **Add** (Hinzufügen), um eine neue Filterliste zu erstellen. Benennen Sie die Filterliste mit **DC replication**. Klicken Sie auf die Schaltfläche **Hinzufügen (Add)**, um einen neuen Filter zu erstellen. Befolgen Sie diese Schritte, um den Assistenten abzuschließen:

- Wählen Sie als Quelladresse **Eigene IP-Adresse (My IP address)** aus.
- Wählen Sie als Zieladresse **Spezielle IP-Adresse** aus, und geben Sie die IP-Adresse des anderen Servers ein.
- Wählen Sie als Protokolltyp **Beliebiger DC (Any)** aus. Dadurch wird der Filter so konfiguriert, dass der gesamte Datenverkehr zwischen den beiden Computern innerhalb von IPsec⁴ übertragen wird.

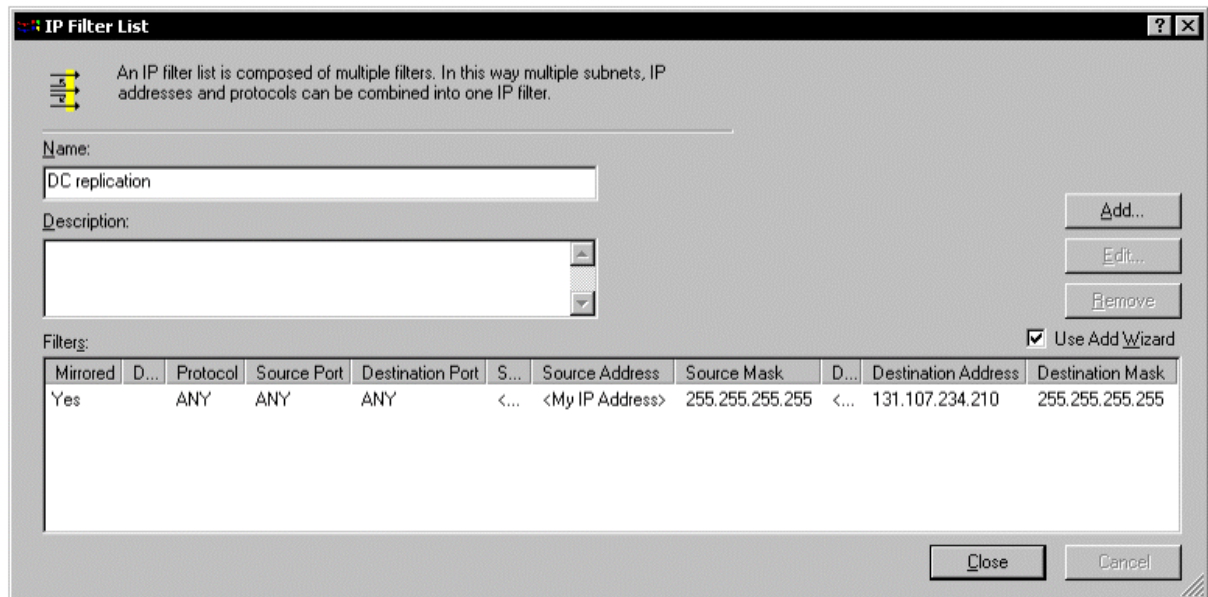


Abbildung 7: Replikationsfilterliste für Domänencontroller

Fügen Sie für die restlichen Domänencontroller weitere Filter hinzu. Schließen Sie anschließend das Dialogfeld.

Als Nächstes legen Sie eine Filteraktion fest. Klicken Sie auf die Registerkarte **Filteraktionen verwalten** und dann auf die Schaltfläche **Hinzufügen**, um eine neue Aktion zu erstellen. Führen Sie im Assistenten die folgenden Schritte aus:

- Benennen Sie die Aktion mit **DC replication**.
- Klicken Sie auf **Sicherheit aushandeln (Negotiate security)**.
- Klicken Sie auf **Keine Kommunikation mit Computern zulassen, die IPSec nicht unterstützen**.
- Klicken Sie auf **Hoch (Encapsulated Secure Payload)**.
- Aktivieren Sie das Kontrollkästchen **Eigenschaften bearbeiten** (Sie müssen später Änderungen vornehmen).
- Klicken Sie auf die Schaltfläche **Fertig stellen**.

Deaktivieren Sie im Dialogfeld **Eigenschaften** das Kontrollkästchen **Unsichere Kommunikation annehmen, aber immer mit IPSec antworten (Accept unsecured communication, but always respond using IPSec)**. Sie möchten verhindern, dass der Server auf unsichere Kommunikation antwortet. Dies gilt natürlich nur für die Computer in der entsprechenden IP-Filterliste. Im Anschluss werden Sie die Filterliste und die Filteraktion mit einer Richtlinie verknüpfen. Schließen Sie alle Dialogfelder.

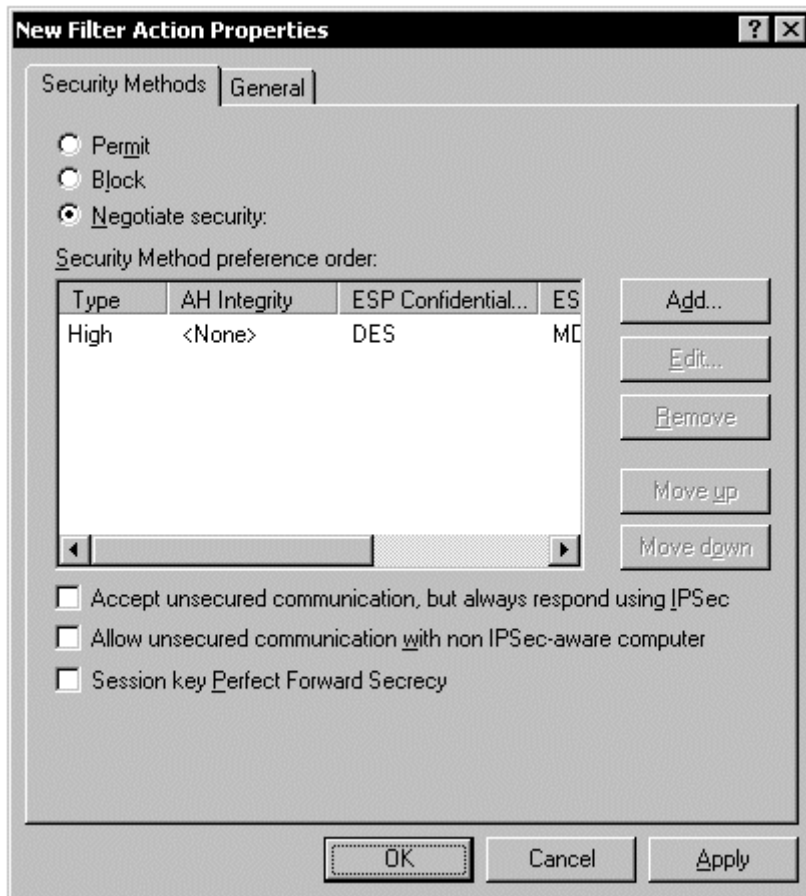


Abbildung 8: Replikationsfilteraktion für Domänencontroller

Nun können Sie die IPSec-Richtlinie erstellen. Klicken Sie im rechten Bereich von MMC mit der rechten Maustaste auf **IP-Sicherheitsrichtlinie erstellen**. Führen Sie im Assistenten die folgenden Schritte aus:

- Benennen Sie die Richtlinie mit **Domain controller replication**.
- Deaktivieren Sie **Die Standardantwortregel aktivieren**.
- Stellen Sie sicher, dass das Kontrollkästchen **Eigenschaften bearbeiten** aktiviert ist, und schließen Sie den Assistenten.

Die Richtlinie ist nun vorhanden, enthält jedoch keine Regeln.

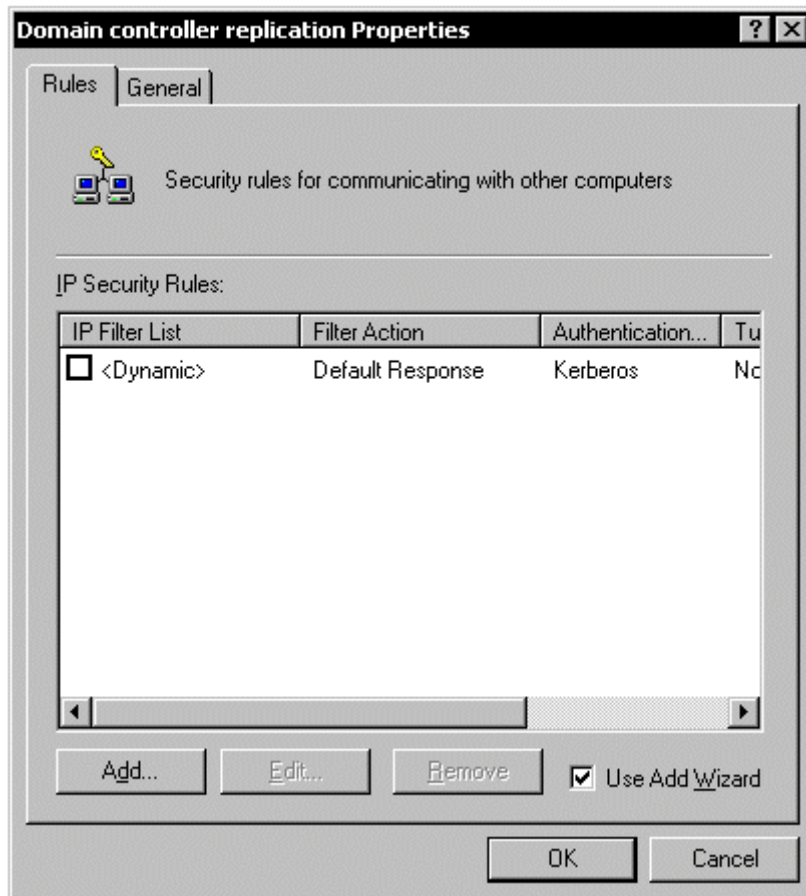


Abbildung 9: IPSec-Replikationsrichtlinie für Domänencontroller

Sie erstellen eine Regel, indem Sie die zuvor erstellte Filterliste mit der Filteraktion verknüpfen. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Regel zu definieren. Führen Sie im Assistenten die folgenden Schritte aus:

- Aktivieren Sie **Diese Regel spezifiziert keinen Tunnel**.
- Wählen Sie als Netzwerktyp **LAN** aus.

Wählen Sie eine Authentifizierungsmethode.

- Wählen Sie **Windows 2000-Standard (Kerberos V5-Protokoll)** aus, wenn Sie für DCPROMO PPTP-Tunnel verwendet haben, *oder*
- Wählen Sie **Verwenden eines Zertifikats von dieser Zertifizierungsstelle** aus, wenn Sie Zertifikate verwendet haben. Klicken Sie dann auf **Durchsuchen**, und wählen Sie die Zertifizierungsstelle aus, die das auf dem Computer installierte Computerzertifikat ausgegeben hat.
- Es wird eine Liste mit IP-Filterlisten angezeigt. Wählen Sie in der Liste die zuvor erstellte Filterliste **DC replication** aus.
- Es wird eine Liste mit IP-Filteraktionen angezeigt. Wählen Sie in der Liste die zuvor erstellte Filteraktion **DC replication** aus.
- Bearbeiten Sie keine Eigenschaften. Beenden Sie den Assistenten.

Die Richtlinie sieht nun so aus (die Spalte **Authentifizierung [Authentication]** zeigt **Zertifikat** an, wenn Sie diese Methode ausgewählt haben).

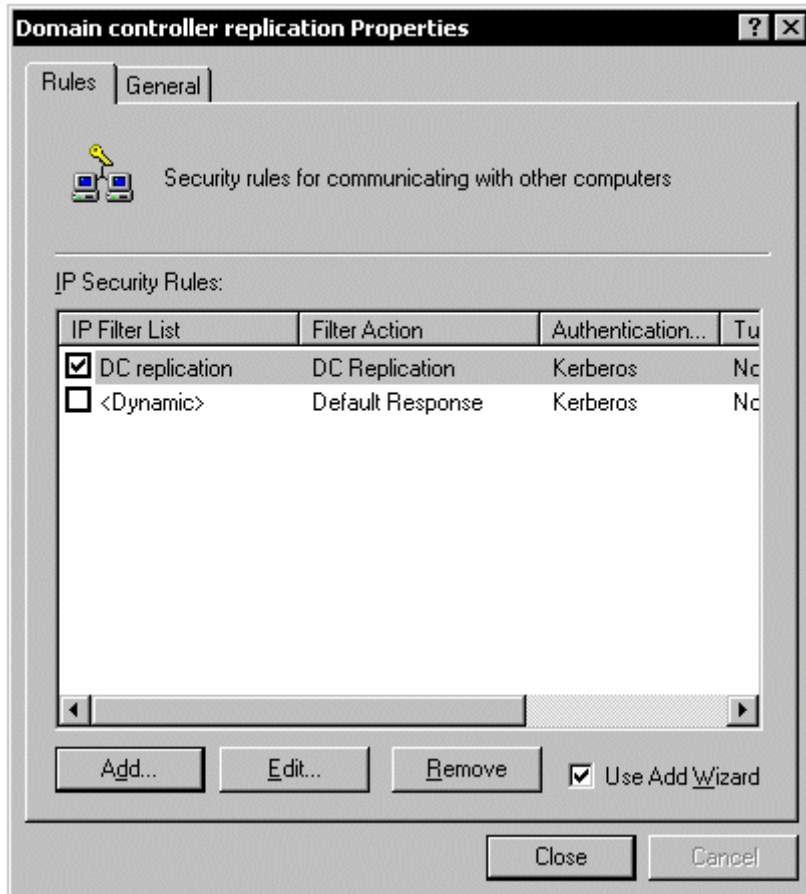


Abbildung 10: Vervollständigte Replikationsrichtlinie für Domänencontroller

Zuletzt müssen Sie die Richtlinie zuweisen.

- Klicken Sie mit der rechten Maustaste auf die Richtlinie **Domain controller replication**.
- Klicken Sie auf **Zuweisen**.

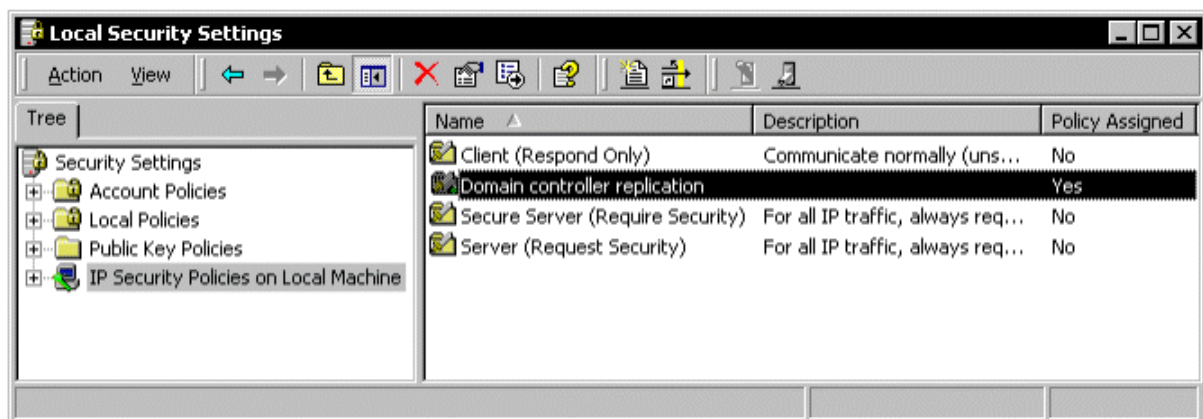


Abbildung 11: Zugewiesene Domänencontrollerrichtlinie

Die IPSec-Verarbeitung setzt sofort ein, ohne dass der Server neu gestartet werden muss.

Für jeden Domänencontroller ist eine ähnliche IPSec-Richtlinie erforderlich. Unabhängig davon, ob sich der Domänencontroller im internen Netzwerk, der DMZ oder dem externen Netzwerk befindet, müssen Sie seine IPSec-Richtlinie so konfigurieren, dass sämtliche Kommunikation mit allen anderen Domänencontrollern IPSec durchläuft. Dies ermöglicht nicht nur, dass die Konsistenzprüfung (Knowledge Consistency Checker, KCC) eine Replikationstopologie erstellt, die den Firewall ignoriert, sondern schützt auch die gesamte IPSec-Replikation zwischen allen Servern.

Testen der IPSec-Richtlinie. Sie sollten die erstellten Richtlinien testen. Nachdem Sie eine Richtlinie auf mindestens zwei Computern erstellt und zugewiesen haben, können Sie mithilfe des Dienstprogramms **IPSECMON.EXE** überprüfen, wann die Computer die IPSec-Sicherheitszuordnungen einrichten:

- Öffnen Sie ein Befehlsfenster.
- Rufen Sie den Befehl **ipsecmom** auf. Ein grafisches Dienstprogramm wird gestartet, das die aktuellen Sicherheitszuordnungen und den Umfang des authentifizierten und/oder verschlüsselten Datenverkehrs auflistet, der den Server durchlaufen hat. (Es gibt zu diesem Zeitpunkt wahrscheinlich keine Systemadministratoren, es sei denn, die Domänencontroller haben mit dem Informationsaustausch begonnen.)
- Klicken Sie auf die Schaltfläche **Optionen**, und ändern Sie die Aktualisierungsrate in 1 Sekunde.
- Wechseln Sie zurück zur Befehlseingabeaufforderung, und rufen Sie den PING-Befehl auf einem anderen Domänencontroller auf, der ebenfalls über eine IPSec-Richtlinie verfügt. Verwenden Sie den Parameter **-t**, um den PING-Befehl bis zum Abbruch fortlaufend aufzurufen (**ping -t ip-address**).
- Suchen Sie nach mehreren Antworten zu **IP-Sicherheit wird verhandelt**. Die Computer tauschen kryptografische Schlüssel aus und erstellen ihre Sicherheitszuordnungen. Schließlich werden normale Antworten angezeigt. Es dauert ca. 10-12 Sekunden, um die Sicherheitszuordnungen in beide Richtungen einzurichten.
- Drücken Sie STRG +C, um den Vorgang abubrechen.

Weiteres Sperren von Domänencontrollern in einer DMZ

Netzwerke mit Unterstützung von E-Commerce- und Extranetverbindungen benötigen u. U. einen Domänencontroller in der DMZ. Wenn es den Anschein hat, dass dadurch Sicherheitsprobleme erzeugt werden, kann IPSec auch hier von Nutzen sein. Mithilfe der Features zum Zulassen und Ablehnen von IPSec-Regeln können detailliert abgestufte Paketfilter erstellt werden. Weitere Informationen finden Sie im Dokument "Using IPSec to Lock Down a Server" unter <http://www.microsoft.com/ISN/Columnists/P66703.asp> (englischsprachig). Sie können die dort angegebene Methode mit den hier vorgestellten Informationen kombinieren, um eine IPSec-Richtlinie zu erstellen, die nur eine sichere Kommunikation zwischen Domänencontrollern erlaubt und sämtlichen anderen Datenverkehr am Erreichen des Domänencontrollers in der DMZ hindert.

Ist dies eine gerechtfertigte Verwendung von IPSec?

Obwohl dies von den IPSec-Entwicklern nicht vorgesehen war, hat sich das Protokoll zu einer ausgezeichneten Methode zum Kapseln komplexen Datenverkehrs entwickelt, damit dieser sicher zwischen Netzwerken transportiert werden kann. Mit dem IPSec-Richtlinienmodul in Windows 2000 können Sie sehr detailliert abgestufte Regeln erstellen, die Datenverkehr angeben, der zwischen Hosts erlaubt, blockiert oder geschützt wird. In diesem Szenario wird das Modul zum Schutz des gesamten Datenverkehrs zwischen bekannten Hosts bzw. bestimmten Domänencontrollern verwendet, während anderer ein- und ausgehender Datenverkehr dieser Hosts zugelassen wird.

Weitere Informationen zu Windows 2000 IPSec und anderen Sicherheitsfeatures von Windows 2000 finden Sie unter <http://www.microsoft.com/windows2000/technologies/security/default.asp> (englischsprachig) und <http://www.microsoft.com/technet/security/> (englischsprachig).

1 TCP wird für Zonenübertragungen und Antworten auf Anforderungen mit mehr als 512 Bytes verwendet.

2 Vorinstallierte Schlüssel werden in diesem Dokument nicht behandelt. Die Authentifizierung mithilfe vorinstallierter Schlüssel ist in Windows 2000 nur aus Gründen der Kompatibilität mit anderen IPSec-Implementierungen und der Entsprechung mit RFCs zu IPSec enthalten. Von der Verwendung vorinstallierter Schlüssel in einer Produktionsumgebung wird aufgrund der inhärenten Sicherheitsrisiken dringend abgeraten, die mit der shared-secret style-Authentifizierung einhergehen.

3 Wenn Sie sich anstatt für die Kerberos- für die IPSec-Authentifizierung entscheiden, können Sie die Server so konfigurieren, dass Kerberos-Datenverkehr innerhalb von IPSec übertragen wird. Dies wird weiter unten ausführlicher besprochen. Ungeachtet des Authentifizierungsmodus ist Kerberos zwischen Domänencontrollern weiterhin erforderlich.

4 Das heißt, der gesamte Datenverkehr, mit Ausnahme des von der IPSec-Verarbeitung nicht berücksichtigten Datenverkehrs, wie bereits zuvor besprochen.